

McCORRISTON MILLER MUKAI MACKINNON LLP

WILLIAM C. McCORRISTON #995-0
DAVID J. MINKIN #3639-0
Five Waterfront Plaza, 4th
Floor500 Ala Moana
Boulevard Honolulu, Hawai'i
96813
Telephone: 808.529.7300
Facsimile: 808.535.8056

E-Mail: mccorriston@m4law.com; minkin@m4law.com

JAMES A. BRYANT (*pro hac vice*)
The Cochran Firm California
4929 Wilshire Blvd., Suite 1010
Los Angeles, CA 90010
Telephone: 323-435-8205
Facsimile: 310-802-3829
E-mail: jbryant@cochranfirm.com

Attorneys for Defendant
NICKIE MALI LUM DAVIS

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF HAWAII

UNITED STATES OF AMERICA,

Plaintiff,

vs.

NICKIE MALI LUM DAVIS;

Defendant.

CR. NO. 20-00068 LEK

INDEX OF EXHIBITS

INDEX OF EXHIBITS

1. A true and correct copy of the email communication between Abbe Lowell and John Keller dated August 9, 2020 is attached hereto as Exhibit A.
2. A true and correct copy of the email communication between Abbe Lowell and John Keller dated August 10, 2020 is attached hereto as Exhibit B.
3. A true and correct copy of the email communication between Abbe Lowell and John Keller dated August 10, 2020 re: Status Call is attached hereto as Exhibit C.
4. A true and correct copy of the email communication between Abbe Lowell and John Keller dated August 10, 2020 re: Lum Davis Plea Colloquy is attached hereto as Exhibit D.
5. A true and correct copy of compilation of DOJ press releases related to cases involving Scott A. Claffee is attached hereto as Exhibit E.
6. A true and correct copy of compilation of DOJ press releases related to cases involving Ian C. Richardson is attached hereto as Exhibit F.
7. A true and correct copy a Department Justice Press Release re: China Initiative is attached hereto as Exhibit G.
8. A true and correct copy of the email communication between Ian Richardson and John Keller dated January 19, 2021 is attached hereto as Exhibit H.
9. A true and correct copy of the email communication between Abbe

Lowell and John Keller dated August 13, 2020 is attached hereto as Exhibit I.

10. A true and correct copy of the email communication between Abbe Lowell and John Keller dated August 15, 2020 is attached hereto as Exhibit J.

11. A true and correct copy of the email communication between Abbe Lowell and John Keller dated August 15, 2020 is attached hereto as Exhibit K.

12. A true and correct copy of the email communication between Abbe Lowell and John Keller dated August 20, 2020 is attached hereto as Exhibit L.

13. A true and correct copy of the email communication between Abbe Lowell and John Keller dated August 12, 2020 is attached hereto as Exhibit M.

DATED: Los Angeles, California, May 17, 2022.

Isl James A. Bryant
JAMES A. BRYANT

EXHIBIT A

From: [Keller, John \(CRM\)](#)
To: [Lowell, Abbe](#); [Mulryne, Sean \(CRM\)](#)
Cc: [Porter, Jennie](#); [Man, Christopher](#)
Subject: RE: FRCrP 11 and FRE 408, 410 Communication
Date: Sunday, August 9, 2020 6:00:00 PM

Thanks for the quick response, Abbe. In your discussions with your client on forfeiture please try to get us as many specifics and documentary corroboration as you can on the money that she received. Given that we all now know that Pras Michel received the \$10 million in August 2017 in furtherance of the Low/Guo conduct, and that he entered into the entertainment contract with your client as a pretext (at least from his perspective), what would be the basis of her “innocent owner” claim to the \$7.5 million that she received? Or put differently, what evidence is there that she did anything for the money other than contribute to the group’s efforts on Low and Guo, or anything that would justify such a large payment?

From: Lowell, Abbe <ADLowell@winston.com>
Sent: Sunday, August 9, 2020 5:49 PM
To: Keller, John (CRM) <John.Keller@CRM.USDOJ.GOV>; Mulryne, Sean (CRM) <Sean.Mulryne@CRM.USDOJ.GOV>
Cc: Porter, Jennie <JPPorter@winston.com>; Man, Christopher <CMan@winston.com>
Subject: RE: FRCrP 11 and FRE 408, 410 Communication

Thanks for sending this and I will forward. I am still afraid that your view of the forfeiture will be the deal breaker (which we both agree is a shame). I will try to arrange a call with our client tonight but, if not, as early tomorrow as we can.

Abbe

Abbe David Lowell

Partner

Winston & Strawn LLP
1901 L Street, N.W.
Washington, DC 20036

D: +1 202-282-5875

F: +1 202-282-5100

200 Park Avenue
New York, NY 10166-4193

D: +1 212-294-3305

F: +1 212-294-4700

[VCard](#) | [Email](#) | [winston.com](#)

WINSTON
& STRAWN
LLP

EXHIBIT B

From: [Keller, John \(CRM\)](#)
To: [Lowell, Abbe](#); [Mulryne, Sean \(CRM\)](#)
Cc: [Porter, Jennie](#); [Man, Christopher](#); "mccorrison@m4law.com"
Subject: RE: F.R.Cr.P. 11 and F.R.Evid. 408, 410 Communication
Date: Monday, August 10, 2020 12:31:00 PM

Abbe,

Thank you for your prompt list of activities that your client contends were undertaken for the \$7.5 million that she received from Pras Michel in September 2017 and some of the underlying documents.

It appears that Ms. Lum Davis did relatively little in the months leading up to and following the \$7.5 million payment from Pras Michel in furtherance of any entertainment venture. In contrast, Ms. Lum Davis was extremely active at that time on the conspirators' efforts to facilitate the removal of Guo Wengui on Low and Sun's behalf.

These conversations would perhaps be more productive on a call.

Let's discuss after you have had time to discuss with your client. Let us know if there is a convenient time this afternoon.

-John

From: Lowell, Abbe <ADLowell@winston.com>
Sent: Monday, August 10, 2020 12:15 PM
To: Keller, John (CRM) <John.Keller@CRM.USDOJ.GOV>; Mulryne, Sean (CRM) <Sean.Mulryne@CRM.USDOJ.GOV>
Cc: Porter, Jennie <JPPorter@winston.com>; Man, Christopher <CMan@winston.com>; 'mccorrison@m4law.com' <mccorrison@m4law.com>
Subject: F.R.Cr.P. 11 and F.R.Evid. 408, 410 Communication

John and Sean –

The premise of your proposal on forfeiture is your view that *all* the payments by Pras to Ms. Davis were either for the first or second effort (and none related to any entertainment venture). We have demonstrated the differences between the two foreign efforts from her perspective. Among other things, it was clear at the time that Person B had and was promoting his own financial interests and reasons (with there not being a commission deal for any of that), and now it is clear that Person A had a side deal with Foreign National A to help on the second matter that Ms. Davis did not know at the time. The screen shots you sent also show that Person H was not shy about mentioning his business interests in the region and I think he is not even being asked to plead or face charges. Ms. Davis had clear and admitted financial interests in helping Foreign National A and continues to assert, other than making sure that Foreign National A was pleased so he would pay the amount they expected on his

case, that she did not have any arrangement for finances for the second matter. This is why I have tried to find language where she can include her efforts on the second matter in the charge but in a different way and different language. She cannot admit to an offense for that in the same manner that she can for the other.

From your starting point that the two matters are the same as to her, you then proceed to your view of the amount in forfeiture and that continues the disconnect. Unrealistic or not in retrospect, Ms. Davis believed at the time that she and Pras had an agreement for \$150 MM for entertainment ventures to be funded by another person. Given the amounts involved in promoting and producing movies, videos, music, and what other investments she heard were being made from investors in that part of the world, this was not a crazy number. When she got the funds from Pras not linked to the funds going to Colfax as well, to her it was part of that arrangement.

She will admit where she crossed the line on the first and forfeit the net proceeds of that effort. That is fair. More is really not. Cases we have seen (*U.S. v. Ben Israel*, *U.S. v. Siljander*) provide a great deal of discretion and those that had forfeiture (*U.S. v. Park*) usually have other factors – trials v. plea and cooperation, additional charges, etc.

There are not scores of cases, but that means there is more room here as well. And I do not see any of them having the type of cooperation our client has provided and could provide.

And as to her perspective, here is a timeline of the entertainment venture compared to the \$833K and \$7.5 million payments. I have uploaded some of the relevant documents to an FTP, which you can access here:

Link: <https://mft.winston.com/?ShareToken=A63A77FB5F287A0A0939DD75A74BEB093070EE0E>
Password: 271M7XTV

- Nickie and Pras had a history of working together. As one example, in 2013, Nickie flew to Haiti because of some work with him.
- May 3, 2017: While in Bangogk, Pras mentions the entertainment venture and tells Nickie he wants to split it with her.
- August 9, 2017: Nickie emails wire instructions for her business account with the subject “see attached wire instructions for loan investment.” Tab 1.
- August 9, 2017: Pras transfers \$833K to Nickie
- August 10, 2017: Tricia Davis (who is involved with Pras and Nickie on entertainment ventures) emailed saying her deal was 10% off the top and as of that day, Pras sent only \$50K. Tab 2.
- September 1, 2017: Nickie emails Pras wire instructions for her business account with the subject “Wire for payment”. Tab 3.

- September 5, 2017: Promissory Note executed between Nickie and Artemus. Tab 4.
- September 5, 2017: Pras transfers \$7.5 million to Nickie.
- September 18, 2017: Consulting agreement between Nickie and Anicorn signed. Tab 5.

And then, as to her efforts, here is a partial list of what both prompted the agreement and her follow-up:

- December 2016: Draft agreement between LVM Pictures, Inc. and Foxy Brown Productions Inc. re Vivica Fox Talk Show. Tab 6.
- April 21, 2017: Nickie is forwarded an email attaching two demos from a famous actress in China who wants to produce an album. Tab 7.
- April 23, 2017: Nickie is forwarded an email about the CMA Festival and a Chinese singer who could perform at it. Tab 8.
- May 3, 2017: While in Bangokk, Pras mentions the entertainment venture and tells Nickie he wants to split it with her.
- December 17, 2017: Pras emails Nickie a link to his Sweet Micky documentary. Tab 9.
- January 11, 2018: Nickie emails Pras re "SEVERRINC, LLC Convertible Bridge Note - Draft" and asks about an agreement with executive producer credits and company credits, etc. Tab 10.
- January 12, 2018: Nickie emails Neville Richardson and Pras re GIVE TV Promissory Note and asks about the production company credits and executive producer credits. Tab 11.
- April 16, 2018: Nickie receives an email from James Bryant re a potential investment into "GameON" (an app). Tab 12.
- April 16, 2018: Pras send to Nickie a draft financing agreement between Prosperity and LNS to develop two theatrical feature pictures entitled Johnny Nicholas and Under Cover Hip Hop Cop. Tab 13.
- April 20, 2018: Email from Nickie to James Bryant re revision of contract between DeJuan Turrentine and Nickie and Trisha. Tab 14.
- July 10, 2018: Draft equity distribution agreement between TRINICK and Roc Nation Records. Tab 15.
- August 22, 2018: Email thread of James Bryant introducing the artist "Sofi Greene" to Nickie and Trisha because of their "direct relationship with Roc Nation". Tab 16.
- September 13, 2018: Email from James Bryant re final operating contract for TRINICK. Tab 17.
- September 25, 2018: Email chain with Davis, Trisha, and James Bryant re TRINICK Roc Nation Equity Contract and artist distribution license agreement with JP CaliSmoov. Tab 18.

We have been and are reviewing the drafts with Ms. Davis and we should have a call after that and after you have reviewed this email to further discuss the issues of the offense v. the forfeiture amount and other open issues.

Thank you for the effort and consideration,

Abbe

Abbe David Lowell

Partner

Winston & Strawn LLP
1901 L Street, N.W.
Washington, DC 20036

D: +1 202-282-5875

F: +1 202-282-5100

200 Park Avenue
New York, NY 10166-4193

D: +1 212-294-3305

F: +1 212-294-4700

[VCard](#) | [Email](#) | [winston.com](#)



The contents of this message may be privileged and confidential. If this message has been received in error, please delete it without reading it. Your receipt of this message is not intended to waive any applicable privilege. Please do not disseminate this message without the permission of the author. Any tax advice contained in this email was not intended to be used, and cannot be used, by you (or any other taxpayer) to avoid penalties under applicable tax laws and regulations.

EXHIBIT C

From: [Keller, John \(CRM\)](#)
To: [Lowell, Abbe](#)
Cc: [Mulryne, Sean \(CRM\)](#); [Porter, Jennie](#); [Man, Christopher](#); mccorriston@m4law.com
Subject: Re: Status Call
Date: Monday, August 10, 2020 12:57:59 PM

Works for me. Sean?

On Aug 10, 2020, at 12:56 PM, Lowell, Abbe <ADLowell@winston.com> wrote:

To account for the time difference and to see if Mac can join, can we talk at 3 PM?

Abbe David Lowell

Partner

Winston & Strawn LLP
1901 L Street, N.W.
Washington, DC 20036
D: +1 202-282-5875
F: +1 202-282-5100

200 Park Avenue
New York, NY 10166-4193
D: +1 212-294-3305
F: +1 212-294-4700

[VCard](#) | [Email](#) | winston.com

<image001.jpg>

The contents of this message may be privileged and confidential. If this message has been received in error, please delete it without reading it. Your receipt of this message is not intended to waive any applicable privilege. Please do not disseminate this message without the permission of the author. Any tax advice contained in this email was not intended to be used, and cannot be used, by you (or any other taxpayer) to avoid penalties under applicable tax laws and regulations.

EXHIBIT D

Shawne Honda

From: Keller, John (CRM) <John.Keller2@usdoj.gov>
Sent: Friday, August 28, 2020 10:17 AM
To: Lowell, Abbe; Sorenson, Ken (USAHI); William C. McCorriston
Cc: William C. McCorriston
Subject: RE: Lum Davis Plea Colloquy

I think the primary point is that it would likely be helpful to have some precise language available to Ms. Lum Davis for her to rely on in admitting what she did and specifically, her awareness of FARA and deliberate avoidance of raising the issue after it became clear that their conduct required registration.

From: Lowell, Abbe <ADLowell@winston.com>
Sent: Friday, August 28, 2020 4:05 PM
To: Keller, John (CRM) <John.Keller@CRM.USDOJ.GOV>; Sorenson, Ken (USAHI) <KSorenson@usa.doj.gov>; William C. McCorriston <WMcCorriston@m4law.com>
Cc: mccorriston@m4law.com
Subject: RE: Lum Davis Plea Colloquy

Over the past weeks, John and I had spoken about the element of willfulness. The best description of that is her willful blindness after the issue of FARA was raised and she went along with what she was told when she thought it was wrong. Her saying she knew she was aiding and abetting others to act on behalf of a foreign principal is not an issue, I think. She surely knew that acting on behalf of such a person required disclosure unless it was exempted and then that is where her willful blindness comes in. Is that what you mean?

Abbe David Lowell

Partner

Winston & Strawn LLP
1901 L Street, N.W.
Washington, DC 20036
D: +1 202-282-5875
F: +1 202-282-5100

200 Park Avenue
New York, NY 10166-4193
D: +1 212-294-3305
F: +1 212-294-4700

VCard | Email | winston.com

**WINSTON
& STRAWN**
LLP

From: Keller, John (CRM) <John.Keller2@usdoj.gov>
Sent: Friday, August 28, 2020 4:00 PM
To: Sorenson, Ken (USAHI) <Ken.Sorenson@usdoj.gov>; Lowell, Abbe <ADLowell@winston.com>; William C. McCorriston <WMcCorriston@m4law.com>

Cc: mccorriston@m4law.com

Subject: RE: Lum Davis Plea Colloquy

Thanks, Ken. I agree wholeheartedly and made a similar suggestion this morning.

From: Sorenson, Ken (USAHI) <KSorenson@usa.doj.gov>

Sent: Friday, August 28, 2020 3:57 PM

To: Keller, John (CRM) <John.Keller@CRM.USDOJ.GOV>; adlowell@winston.com; William C. McCorriston <WMcCorriston@m4law.com>

Cc: mccorriston@m4law.com

Subject: RE: Lum Davis Plea Colloquy

Gents: The following advice is completely gratuitous and probably worth about every cent you paid for it. ☺ For what it's worth, I find it helpful in cases such as this, where intent is such a critical element, for counsel to prepare some form of written statement for the defendant to use as a guide, or even a script, during the Rule 11 colloquy. The court (with the assistance of defense counsel) can work its way through a few hick-ups, but at times (as we all know) a defendant just can't bring themselves to clearly articulate their involvement and culpability. The court will ask Nickie what she did that makes her feel she is guilty of the charged offense and in my general experience this is where things get interesting during the Rule 11 process.

My suggestion that the cleanest way for this portion of the colloquy to proceed would be for Nickie to read from a prepared statement. It doesn't have to be long, and it can incorporate the facts set forth in paragraph 8 of the plea agreement, but the court will want to hear her speak to the offense. Something along the lines of: "I agree with the facts set forth in paragraph 8 of the agreement. I understood that I was acting on behalf of a foreign nation, and a foreign individual, in committing the acts set forth in paragraph 8. I knew and understood that in order to perform the services I did with respect to this matter it was necessary for me to register as an agent of a foreign power with the United States government. I acknowledge that I knowingly failed to so register when performing the services and acts set forth in the plea agreement."

This is only meant as a guide to assist counsel, and if you have better ideas or thoughts about how to handle this portion of the colloquy please act accordingly. I wish everyone a great weekend and good luck on Monday. I'm working through some computer issues at home so I'm hopeful of getting the signature page executed as quickly as possible. TX! Ken

From: Keller, John (CRM) <John.Keller@CRM.USDOJ.GOV>

Sent: Friday, August 28, 2020 2:17 AM

To: adlowell@winston.com; William C. McCorriston <WMcCorriston@m4law.com>

Cc: mccorriston@m4law.com; Sorenson, Ken (USAHI) <KSorenson@usa.doj.gov>

Subject: Lum Davis Plea Colloquy

Abbe and Bill,

I dialed in for a remote plea hearing held by Judge Kobayashi earlier this week (handled by none other than our esteemed colleague, Ken Sorenson). Bill, I'm sure that you and Mac are very familiar with her procedures, but I've attached the notes here in case they are helpful. I'll handle the findings on the harm to the interests of justice justifying the VTC format. But the one critical piece to flag is that the Judge went into some detail with the defendant asking him to state what he did in his own words and following up with factual questions. I realize that I am stepping outside of my lane here, but it may be worth working with Ms. Lum Davis to prepare some specific statements explaining what she did that hits all of the elements, especially willfulness. This may help us avoid things going off of the rails during the actual hearing.

John D. Keller
Principal Deputy Chief
Public Integrity Section
United States Department of Justice
1331 F St. NW | Washington, D.C. 20004
202.598.2231 (Desk) | 202.615.6491 (Cell)

The contents of this message may be privileged and confidential. If this message has been received in error, please delete it without reading it. Your receipt of this message is not intended to waive any applicable privilege. Please do not disseminate this message without the permission of the author. Any tax advice contained in this email was not intended to be used, and cannot be used, by you (or any other taxpayer) to avoid penalties under applicable tax laws and regulations.

EXHIBIT E



THE UNITED STATES ATTORNEY'S OFFICE
NORTHERN DISTRICT *of* NEW YORK

[U.S. Attorneys](#) » [Northern District of New York](#) » [News](#)

Department of Justice

U.S. Attorney's Office

Northern District of New York

FOR IMMEDIATE RELEASE

Thursday, January 30, 2020

Iranian Export Company Executive Sentenced for Violating U.S. Sanctions Against Iran

ALBANY, NEW YORK - Mahin Mojtahedzadeh, age 74, and a citizen of Iran, was sentenced today to time served (443 days in jail) for conspiring to unlawfully export gas turbine parts from the United States to Iran.

The announcement was made by United States Attorney Grant C. Jaquith; James N. Hendricks, Special Agent in Charge of the Albany Field Office of the Federal Bureau of Investigation (FBI); Kevin Kelly, Special Agent in Charge of the Buffalo Field Office of Homeland Security Investigations (HSI); and Jonathan Carson, Special Agent in Charge, the U.S. Department of Commerce, Office of Export Enforcement, New York Field Office.

United States District Judge Mae A. D'Agostino also ordered Mojtahedzadeh to pay a \$5,000 fine. Mojtahedzadeh had been in law enforcement custody since November 14, 2018 and will now be placed into immigration custody for the purposes of removal from the United States.

On July 19, 2019, she pled guilty to one count of conspiring to violate the International Emergency Economic Powers Act (IEEPA) and the Iranian Transactions and Sanctions Regulations. She admitted that she was the President and Managing Director of ETCO-FZC ("ETCO"), an export company with an office in Dubai in the United Arab Emirates. ETCO is a supplier of spare and replacement turbine parts for power generation companies in the Middle East, including Iran.

Mojtahedzadeh admitted that from 2013 through 2017, she worked with companies in Canada and Germany to violate and evade U.S. sanctions against Iran, by having these companies first acquire more than \$3 million dollars' worth of turbine parts from two distributors in Saratoga County, New York.

When the U.S. parts arrived in Canada and Germany, respectively, these companies and Mojtahedzadeh then arranged for the parts to be re-shipped to ETCO's customers in Iran. At all times, U.S. law prohibited the export and re-export of U.S.-origin turbine parts to Iran without a license from the U.S. Office of Foreign Assets Control (OFAC), which neither Mojtahedzadeh nor her co-conspirators possessed.

United States Attorney Grant C. Jaquith stated: "This investigation struck a blow to Iranian efforts to obtain U.S. goods needed for Iran's domestic energy production, and brought to justice three foreign nationals who conspired to circumvent economic sanctions that protect the national security of the United States."

FBI Special Agent in Charge James N. Hendricks stated: "Anyone looking to evade sanctions and put our nation at risk should be on notice. The FBI, along with our interagency partners, will continue to vigorously investigate these crimes and ensure perpetrators, like Mahin Mojtahedzadeh, are brought to justice."

Kevin Kelly, HSI Buffalo Special Agent in Charge, stated: "The illegal exportation of sensitive and restricted technology is a detriment to our national security. HSI is committed to enforcing these laws and ensuring that safeguards are maintained. The defendant's admission of guilt and the sentence they received today is a clear example of the consequences awaiting those who engage in such actions."

Special Agent in Charge Jonathan Carson, of the U.S. Department of Commerce, Office of Export Enforcement, New York Field Office stated: "We will fully and aggressively enforce our nation's restrictions on exports to Iran. Controls on exports to Iran help apply maximum pressure on Iran to end its promotion of instability and terrorism worldwide. The Office of Export Enforcement will continue to leverage our unique authorities to pursue violators wherever they are, worldwide. We will continue to work with our law enforcement partners to achieve this goal."

Two of Mojtahedzadeh's co-conspirators have previously pled guilty and been sentenced.

Olaf Tepper, a citizen of Germany, pled guilty to conspiring to violate IEEPA. On August 3, 2018, Judge D'Agostino sentenced him to 24 months in prison, and to pay a \$5,000 fine. Tepper was the founder and Managing Director of Energy Republic GmbH ("Energy Republic"), based in Cologne, Germany, which re-exported U.S.-origin turbine parts to Iran, as part of a conspiracy with Mojtahedzadeh.

Mojtaba Biria, a citizen of Germany, also pled guilty to conspiring to violate IEEPA. On August 14, 2019, Judge D'Agostino sentenced him to time served (approximately 21 months in jail). Biria was Energy Republic's Technical Managing Director.

These cases are the result of a joint investigation by FBI, HSI and the Department of Commerce Office of Export Enforcement, and were prosecuted by Assistant U.S. Attorneys Rick Belliss and Michael Barnett, with assistance from Trial Attorney Scott A. Claffee of the Department of Justice's National Security Division, Counterintelligence & Export Control Section.

Topic(s):

Counterintelligence and Export Control

Component(s):

USAO - New York, Northern

Updated January 31, 2020



THE UNITED STATES ATTORNEY'S OFFICE
DISTRICT *of* MASSACHUSETTS

[U.S. Attorneys](#) » [District of Massachusetts](#) » [News](#)

Department of Justice

U.S. Attorney's Office

District of Massachusetts

FOR IMMEDIATE RELEASE

Wednesday, July 22, 2020

Massachusetts Man Sentenced for Illegally Retaining Classified National Defense Information Regarding U.S. Military Programs

BOSTON – A former Raytheon systems engineer was sentenced today for illegally retaining national defense information. The defendant retained 31,000 pages of information that was marked as classified, some of which pertained to U.S. missile defense and was classified at the SECRET level, and altered or obliterated the classification markings on documents.

Ahmedelhadi Yassin Serageldin, 67, of Sharon, was sentenced by U.S. District Court Judge Patti B. Saris to 18 months in prison, one year of supervised release and ordered to pay a fine of \$10,000. In December 2019, Serageldin pleaded guilty to one count of willfully retaining national defense information.

Serageldin was a systems engineer at Raytheon Technologies in Massachusetts from August 1997 until he was terminated in May 2017. Serageldin had a SECRET level security clearance in order to complete his assignments on several defense contracts for the U.S. government involving military radar technology.

After Raytheon raised suspicions to federal authorities about whether Serageldin was being candid during an internal investigation of his computer usage, agents followed Serageldin to a local library where they discovered that he was researching how to delete files from his computer. During the execution of search warrants, over 3,100 electronic files and over 110 paper documents belonging to Raytheon or the Department of Defense, over 570 of which were marked as containing classified information, were recovered. The documents marked as containing classified information totaled approximately 31,000 pages in length. Court documents list five specific documents, all of which pertain to U.S. military programs involving missile defense and are classified at the SECRET level. It was also determined that Serageldin had altered or obliterated the classification markings on approximately 50 documents.

United States Attorney Andrew E. Lelling; Assistant Attorney General John C. Demers of the Justice Department's National Security Division; Joseph R. Bonavolonta, Special Agent in Charge of the Federal Bureau of Investigation, Boston Field Division; and Michael Wiest, Special Agent in Charge of the Naval Criminal Investigative Service, Northeast Field Office made the announcement today. Assistance with the investigation was provided by the Air Force Office of Special Investigations and the Internal Revenue Service's Criminal Investigations in Boston. Raytheon Technologies has cooperated with the investigation, which was launched after they notified federal authorities about the suspicious conduct. Assistant U.S. Attorney Scott L. Garland, Deputy Chief of Lelling's National Security Unit, prosecuted the case with assistance from Trial Attorney Scott Claflie of the Justice Department's National Security Division.


Topic(s):

National Security

Component(s):

USAO - Massachusetts

Updated July 23, 2020

 An official website of the United States government
[Here's how you know](#)



Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Monday, August 17, 2020

Former CIA Officer Arrested and Charged with Espionage

Alexander Yuk Ching Ma, 67, a former Central Intelligence Agency (CIA) officer, was arrested on Aug. 14, 2020, on a charge that he conspired with a relative of his who also was a former CIA officer to communicate classified information up to the Top Secret level to intelligence officials of the People's Republic of China (PRC). The Criminal Complaint containing the charge was unsealed this morning.

Assistant Attorney General for National Security John C. Demers, U.S. Attorney for the District of Hawaii Kenji M. Price, Assistant Director of the FBI's Counterintelligence Division Alan E. Kohler Jr., and Special Agent in Charge of the FBI's Honolulu Field Office Eli S. Miranda made the announcement.

"The trail of Chinese espionage is long and, sadly, strewn with former American intelligence officers who betrayed their colleagues, their country and its liberal democratic values to support an authoritarian communist regime," said Assistant Attorney General for National Security John C. Demers. "This betrayal is never worth it. Whether immediately, or many years after they thought they got away with it, we will find these traitors and we will bring them to justice. To the Chinese intelligence services, these individuals are expendable. To us, they are sad but urgent reminders of the need to stay vigilant."

"The charges announced today are a sobering reminder to our communities in Hawaii of the constant threat posed by those who seek to jeopardize our nation's security through acts of espionage," said U.S. Attorney Price. "Of particular concern are the criminal acts of those who served in our nation's intelligence community, but then choose to betray their former colleagues and the nation-at large by divulging classified national defense information to China. My office will continue to tenaciously pursue espionage cases."

"This serious act of espionage is another example in a long string of illicit activities that the People's Republic of China is conducting within and against the United States," said Alan E. Kohler Jr., Assistant Director of the FBI's Counterintelligence Division. "This case demonstrates that no matter the length or difficulty of the investigation, the men and women of the FBI will work tirelessly to protect our national security from the threat posed by Chinese intelligence services. Let it be known that anyone who violates a position of trust to betray the United States will face justice, no matter how many years it takes to bring their crimes to light."

"These cases are very complicated and take years if not decades to bring to a conclusion," said Eli Miranda, Special Agent in Charge of the FBI's Honolulu Division. "I could not be more proud of the work done by the men and women of the FBI's Honolulu Division in pursuing this case. Their dedication is a reminder that the FBI will never waiver when it comes to ensuring the safety and security of our nation."

Ma is a naturalized U.S. citizen born in Hong Kong. According to court documents, Ma began working for the CIA in 1982, maintained a Top Secret clearance, and signed numerous non-disclosure agreements in which he acknowledged his responsibility and ongoing duty to protect U.S. government secrets during his tenure at CIA. Ma left the CIA in 1989 and lived and worked in Shanghai, China before arriving in Hawaii in 2001.

According to court documents, Ma and his relative (identified as co-conspirator #1) conspired with each other and multiple PRC intelligence officials to communicate classified national defense information over the course of a decade. The scheme began with three days of meetings in Hong Kong in March 2001 during which the two former CIA officers provided information to the foreign intelligence service about the CIA's personnel, operations, and methods of concealing communications. Part of

the meeting was captured on videotape, including a portion where Ma can be seen receiving and counting \$50,000 in cash for the secrets they provided.

The court documents further allege that after Ma moved to Hawaii, he sought employment with the FBI in order to once again gain access to classified U.S. government information which he could in turn provide to his PRC handlers. In 2004, the FBI's Honolulu Field Office hired Ma as a contract linguist tasked with reviewing and translating Chinese language documents. Over the following six years, Ma regularly copied, photographed and stole documents that displayed U.S. classification markings such as "SECRET." Ma took some of the stolen documents and images with him on his frequent trips to China with the intent to provide them to his handlers. Ma often returned from China with thousands of dollars in cash and expensive gifts, such as a new set of golf clubs.

According to court documents, in spring 2019, over the course of two in-person meetings, Ma confirmed his espionage activities to an FBI undercover employee Ma believed was a representative of the PRC intelligence service, and accepted \$2,000 in cash from the FBI undercover as "small token" of appreciation for Ma's assistance to China. Ma also offered to once again work for the PRC intelligence service. On August 12, 2020, during a meeting with an FBI undercover employee before arrest, Ma again accepted money for his past espionage activities, expressed his willingness to continue to help the Chinese government, and stated that he wanted "the motherland" to succeed.

Ma will make his initial appearance before a federal judge tomorrow in the U.S. District Court for the District of Hawaii. He is charged with conspiracy to communicate national defense information to aid a foreign government and faces a maximum penalty of life imprisonment if convicted. The maximum sentence is prescribed by Congress and is provided here for informational purposes. In the event Ma is convicted, a federal district court judge will determine any sentence after taking into account the advisory Sentencing Guidelines and other statutory factors.

The investigation was conducted by the FBI's Honolulu and Los Angeles Field Offices. Assistant U.S. Attorney Ken Sorenson and Trial Attorneys Scott Claffee and Steve Marzen of the National Security Division's Counterintelligence and Export Control Section are prosecuting the case.

Attachment(s):

[Download ma_complaint_.pdf](#)

Topic(s):

Counterintelligence and Export Control
National Security

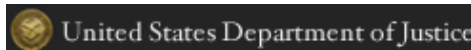
Component(s):

[National Security Division \(NSD\)](#)
[USAO - Hawaii](#)

Press Release Number:

20-789

Updated December 7, 2020



THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT *of* NEW YORK

[U.S. Attorneys](#) » [Eastern District of New York](#) » [News](#)

Department of Justice

U.S. Attorney's Office

Eastern District of New York

FOR IMMEDIATE RELEASE

Monday, September 21, 2020

New York City Police Department Officer Charged with Acting as an Illegal Agent of the People's Republic of China

The Defendant Reported to Officials with the PRC Consulate About the Activities of Chinese Citizens in the New York Area and Assessed Potential Intelligence Sources for the PRC Within the Tibetan Community in New York and Elsewhere

BROOKLYN, NY – A criminal complaint was unsealed today in federal court in Brooklyn charging Baimadajie Angwang, a New York City Police Department officer and United States Army reservist, with acting as an illegal agent of the People's Republic of China (PRC) as well as committing wire fraud, making false statements and obstructing an official proceeding. Angwang was arrested today and will make his initial appearance this afternoon before United States Magistrate Judge Roanne L. Mann.

Seth D. DuCharme, Acting United States Attorney for the Eastern District of New York; John C. Demers, Assistant Attorney General for National Security; Alan E. Kohler, Jr., Assistant Director of the Federal Bureau of Investigation (FBI) Counterintelligence Division; William F. Sweeney, Jr., Assistant Director-in-Charge, Federal Bureau of Investigation, New York Field Office (FBI); and Dermot F. Shea, Commissioner, New York City Police Department (NYPD), announced the arrest and charges.

"The defendant allegedly violated his sworn oath to serve the New York City community and defend the Constitution against all enemies by reporting to PRC government officials about the activities of Chinese citizens in the New York area and developing intelligence sources within the Tibetan community in the United States," stated Acting United States Attorney DuCharme. "This Office, together with our law enforcement partners, remains vigilant in rooting out any attempts at foreign influence through criminal activity taken on behalf of a foreign power in whatever form they may take."

"State and local officials should be aware that they are not immune to the threat of Chinese espionage," said Assistant Attorney General for National Security John C. Demers. "According to the allegations, the Chinese government recruited and directed a U.S. citizen and member of our nation's largest law enforcement department to further its intelligence gathering and repression of Chinese abroad. Our police departments provide for our public safety and are often the first line of defense against the national security threats our country faces. We will continue to work with our state and local partners to protect our nation's great police departments."

"The defendant allegedly violated the trust of his community and the New York City Police Department on behalf of a foreign power, the People's Republic of China. This type of conduct simply cannot be tolerated," stated FBI Assistant Director Kohler. "This case serves as yet another reminder that China represents the biggest

counterintelligence threat to the United States and that the FBI and our partners will be aggressive in investigating and stopping such activities within our nation.”

“This is the definition of an insider threat - as alleged, Mr. Angwang operated on behalf of a foreign government; lied to gain his clearance, and used his position as an NYPD police officer to aid the Chinese government's subversive and illegal attempts to recruit intelligence sources,” stated FBI Assistant Director-in-Charge Sweeney. “The FBI is committed to stopping hostile foreign governments from infiltrating our institutions, and we will we not tolerate the behavior of those who willingly violate their oath to the United States, and covertly work against their fellow citizens. We want to thank the NYPD for its extraordinary partnership on this investigation.”

“As alleged in this federal complaint, Baimadajie Angwang violated every oath he took in this country. One to the United States, another to the U.S. Army, and a third to this Police Department,” stated NYPD Commissioner Shea. “From the earliest stages of this investigation, the NYPD’s Intelligence and Internal Affairs bureaus worked closely with the FBI’s Counterintelligence Division to make sure this individual would be brought to justice.”

According to the publicly filed complaint and the government’s detention memorandum, Angwang, an ethnic Tibetan native of the PRC and naturalized U.S. citizen, is assigned to the NYPD’s community affairs unit where he serves as a liaison to the community served by the 111th Precinct.

Since at least 2014, Angwang allegedly acted at the direction and control of officials at the PRC Consulate in New York City. Specifically, Angwang reported on the activities of Chinese citizens in the New York area, spotted and assessed potential intelligence sources within the Tibetan community in New York and elsewhere, and provided PRC officials with access to senior NYPD officials through invitations to official events. One of the PRC Consular officials at whose direction Angwang acted worked for the China Association for Preservation and Development of Tibetan Culture, a division of the PRC’s United Front Work Department. This Department is responsible for, among other things, neutralizing potential opponents of the PRC and co-opting ethnic Chinese individuals living outside the PRC.

Angwang is also charged with committing wire fraud, making material false statements and obstructing an official proceeding. As part of his employment with the U.S. Army Reserve, Angwang maintained a “SECRET”-level security clearance. According to court documents, in 2019, Angwang completed and electronically submitted an SF-86C form for a background investigation. On the form, Angwang lied by denying that he had contacts with a foreign government or its consulate and by denying that he had close and continuing contacts with foreign nationals, including his family members who live in the PRC, some of whom are affiliated with the People’s Liberation Army.

The charges in the complaint are allegations, and the defendant is presumed innocent unless and until proven guilty. If convicted, Angwang faces a maximum sentence of 55 years’ imprisonment.

The government’s case is being handled by the Office’s National Security and Cybercrime Section. Assistant United States Attorney Michael T. Keilty is in charge of the prosecution, with assistance from Trial Attorney Scott A. Claffee of the National Security Division’s Counterintelligence and Export Control Section.

The Defendant:

BAIMADAJIE ANGWANG

Age: 33

Williston Park, New York

E.D.N.Y. Docket No. 20-MJ-837

Attachment(s):

[Download Angwang Complaint](#)

Topic(s):

National Security

Public Corruption

Component(s):

USAO - New York, Eastern


Contact:

John Marzulli

United States Attorney's Office

(718) 254-6323

Updated September 21, 2020

 An official website of the United States government
[Here's how you know](#)



Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, October 28, 2020

Eight Individuals Charged With Conspiring to Act as Illegal Agents of the People's Republic of China

PRC Officials Directed Multi-Year Campaign of Harassment and Stalking; Directed at U.S. Residents to Force Their Return to PRC

A complaint and arrest warrants were unsealed today in federal court in Brooklyn charging eight defendants with conspiring to act in the United States as illegal agents of the People's Republic of China (PRC). Six defendants also face related charges of conspiring to commit interstate and international stalking. The defendants, allegedly acting at the direction and under the control of PRC government officials, conducted surveillance of and engaged in a campaign to harass, stalk, and coerce certain residents of the United States to return to the PRC as part of a global, concerted, and extralegal repatriation effort known as "Operation Fox Hunt."

Zhu Yong, Hongru Jin, and Michael McMahon were arrested today and will be arraigned this afternoon via teleconference before U.S. Magistrate Judge Peggy Kuo. Rong Jing and Zheng Congying were arrested in the Central District of California, and their initial appearances will take place in that district later today. Zhu Feng, Hu Ji, and Li Minjun remain at large.

"With today's charges, we have turned the PRC's Operation Fox Hunt on its head — the hunters became the hunted, the pursuers the pursued," said Assistant Attorney General for National Security John C. Demers. "The five defendants the FBI arrested this morning on these charges of illegally doing the bidding of the Chinese government here in the United States now face the prospect of prison. For those charged in China and others engaged in this type of conduct, our message is clear: stay out. This behavior is not welcome here."

"The Chinese government's brazen attempts to surveil, threaten, and harass our own citizens and lawful permanent residents, while on American soil, are part of China's diverse campaign of theft and malign influence in our country and around the world," said FBI Director Christopher Wray. "The FBI will use all of its tools to investigate and defeat these outrageous actions by the Chinese government, which are an affront to America's ideals of freedom, human rights, and the rule of law."

"As alleged, the defendants assisted PRC officials in a scheme to coerce targeted individuals to return to the PRC against their will," said Acting U.S. Attorney Seth D. DuCharme. "The United States will not tolerate the conduct of PRC carrying out state-authorized actions on U.S. soil without notice to, and coordination with, the appropriate U.S. authorities. Nor will we tolerate the unlawful harassment and stalking of U.S. residents to further PRC objectives." Acting U.S. Attorney DuCharme also extended his thanks and appreciation to the FBI's Los Angeles Field Office for their work on the case.

"Today's announcement of these charges further highlights the FBI's ongoing and aggressive commitment to investigate China's efforts to illegally impose its will in the United States", said Special Agent in Charge George M. Crouch Jr. of the FBI Newark Field Office. "This case should serve as a reminder to the People's Republic of China that when it directs criminal activity within our borders, the FBI and its law enforcement partners will make sure the perpetrators are held accountable."

"The worldwide presence and investigative capabilities of the Diplomatic Security Service enables us to work with our law enforcement partners domestically and around the world to bring criminals to justice," said Keith Byrne, Special Agent in Charge of the New York Field Office of the Diplomatic Security Service.

According to the complaint, the defendants participated in an international campaign to threaten, harass, surveil and intimidate John Doe-1, a resident of New Jersey, and his family in order to force them to return to the PRC as part of an international effort by the PRC government known within the PRC as “Operation Fox Hunt” and “Operation Skynet.” In furtherance of the operation, the PRC government targets Chinese individuals living in foreign countries that the PRC government alleges have committed crimes under PRC law and seeks to repatriate them to the PRC to face charges. Rather than rely upon proper forms of international law enforcement cooperation, such as Interpol “red notices” and requests for information through appropriate governmental channels, the defendants allegedly engaged in clandestine, unsanctioned, and illegal conduct within the United States and facilitated the travel of PRC government officials (PRC Officials) to U.S. soil in order to further carry out these illegal acts. Between 2016 and 2019, multiple PRC Officials directed the defendants, and several others, to engage in efforts to coerce the victims to return to the PRC, which included the following:

Surveillance and Coercion

In April 2017, defendants Zhu Feng, Hu Ji, Li Minjun, Hongru Jin, Zhu Yong, and Michael McMahon, together with others, including the PRC Officials, allegedly participated in a scheme to bring John Doe-1’s elderly father from the PRC to the United States against the father’s will and to use the surprise arrival of his elderly father to threaten and attempt to coerce John Doe-1’s return to the PRC. Zhu Feng, Hu Ji, and Zhu Yong worked with Michael McMahon, a private investigator, to gather intelligence about and locate John Doe-1 and his wife in the United States. PRC Officials coerced the father of John Doe-1 to travel from the PRC to the New York area in the company of Li Minjun, a doctor, who traveled with the elderly father from the PRC to the New York area. Hongru Jin assisted with logistics of the operation when Zhu Feng, Li Minjun, John Doe-1’s elderly father, and other PRC officials arrived in the U.S.

As charged in the complaint, during this phase of the scheme, McMahon, whose task was to surveil John Doe-1’s father in order to locate John Doe-1 and his wife, suggested to Zhu Feng that they could “harass [John Doe-1]. Park outside his home and let him know we are there.” Later, Zhu Feng told McMahon, “[t]hey definitely grant u a nice trip if they can get [John Doe-1] back to China haha.”

The conspirators also discussed the false statements John Doe-1’s father should make to U.S. immigration authorities about the purpose of his travel to the United States. The conspirators also made efforts to destroy evidence and delete their electronic communications to avoid detection by U.S. law enforcement.

Targeting and Harassment of Victims’ Daughter

Between May 2017 and July 2018, Rong Jing and several co-conspirators allegedly targeted John Doe-1’s adult daughter for surveillance and online harassment. Specifically, Rong Jing attempted to hire a private investigator to locate John Doe-1’s adult daughter in order to photograph and video record the daughter as part of a campaign to exert pressure on John Doe-1. Around the same time, an unidentified co-conspirator sent harassing messages over social media to John Doe-1’s daughter and her friends related to the PRC’s interest in repatriating John Doe-1.

Continued Harassment of Victims

In September 2018, Zheng Congying and another unidentified co-conspirator allegedly affixed a threatening note to the door of the John Doe-1’s residence stating, “If you are willing to go back to mainland and spend 10 years in prison, your wife and children will be all right. That’s the end of this matter!” Between February 2019 and April 2019, other co-conspirators caused unsolicited packages to be sent to John Doe-1’s residence. These packages contained letters and a video with messages intended to coerce John Doe-1’s return to the PRC by threatening harm to family members still residing in the PRC.

The charges in the complaint are allegations, and the defendants are presumed innocent unless and until proven guilty. If convicted of the charged conspiracy to act as an agent of the PRC, each of the eight defendants charged today faces a maximum sentence of five years in prison. Defendants Zhu Feng, Hu Ji, Li Minjun, Michael McMahon, Rong Jing, and Zheng Congying also face an additional charge of conspiracy to commit interstate and international stalking, which carries a maximum sentence of five years in prison.

The government’s case is being handled by the Office’s National Security and Cybercrime Section. Assistant U.S. Attorneys Craig R. Heeren and J. Matthew Haggans are in charge of the prosecution, with assistance from Trial Attorney Scott A. Claffee of the National Security Division’s Counterintelligence and Export Control Section.

Attachment(s):

[Download 2020_10_28_fox_hunt_complaint.pdf](#)

[Download china_arrest_graphic_1.jpg](#)

[Download china_arrest_graphic_2.jpg](#)

[Download china_arrest_graphic_3.jpg](#)

[Download china_arrest_graphic_4.jpg](#)

Topic(s):

National Security

Component(s):

[National Security Division \(NSD\)](#)

Press Release Number:

20-1170

Updated October 29, 2020



THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT *of* NEW YORK

[U.S. Attorneys](#) » [Eastern District of New York](#) » [News](#)

Department of Justice

U.S. Attorney's Office

Eastern District of New York

FOR IMMEDIATE RELEASE

Friday, December 18, 2020

**China-Based Executive at U.S. Telecommunications Company
Charged with Disrupting Video Meetings Commemorating
Tiananmen Square Massacre**

**Defendant Coordinated with the PRC Government to Target Dissidents and Disrupt
Meetings**

A complaint and arrest warrant were unsealed today in federal court in Brooklyn charging Xinjiang Jin, also known as "Julien Jin," with conspiracy to commit interstate harassment and unlawful conspiracy to transfer a means of identification. Jin, an employee of a U.S.-based telecommunications company (Company-1) who was based in the People's Republic of China (PRC), allegedly participated in a scheme to disrupt a series of meetings in May and June 2020 held to commemorate the June 4, 1989 Tiananmen Square massacre in the PRC. The meetings were conducted using a videoconferencing program provided by Company-1, and were organized and hosted by U.S.-based individuals, including individuals residing in the Eastern District of New York. Jin is not in U.S. custody.

Seth D. DuCharme, Acting United States Attorney for the Eastern District of New York; John C. Demers, Assistant Attorney General for National Security; and Christopher Wray, Director, Federal Bureau of Investigation (FBI), announced the charges.

"The allegations in the complaint lay bare the Faustian bargain that the PRC government demands of U.S. technology companies doing business within the PRC's borders, and the insider threat that those companies face from their own employees in the PRC," stated Acting United States Attorney DuCharme. "As alleged, Jin worked closely with the PRC government and members of PRC intelligence services to help the PRC government silence the political and religious speech of users of the platform of a U.S. technology company. Jin willingly committed crimes, and sought to mislead others at the company, to help PRC authorities censor and punish U.S. users' core political speech merely for exercising their rights to free expression. The charges announced today make clear that employees working in the PRC for U.S. technology companies make those companies—and their users—vulnerable to the malign influence of the PRC government. This Office will continue working tirelessly to protect against threats to the free expression of political views and religious beliefs, regardless whether those threats come from inside or outside the United States." Mr. DuCharme and Mr. Demers also extended their thanks and appreciation to Company-1 for its cooperation in the government's ongoing investigation.

"No company with significant business interests in China is immune from the coercive power of the Chinese Communist Party," stated Assistant Attorney General Demers. "The Chinese Communist Party will use those within its reach to sap the tree of liberty, stifling free speech in China, the United States and elsewhere about the Party's repression of the Chinese people. For companies with operations in China, like that here, this reality may

mean executives being coopted to further repressive activity at odds with the values that have allowed that company to flourish here.”

“The FBI remains committed to protecting the exercise of free speech for all Americans. As this complaint alleges, that freedom was directly infringed upon by the pernicious activities of Communist China’s Intelligence Services, in support of a regime that neither reflects nor upholds our democratic values,” stated FBI Director Wray. “Americans should understand that the Chinese Government will not hesitate to exploit companies operating in China to further their international agenda, including repression of free speech.”

According to the complaint, Jin served as Company-1’s primary liaison with PRC law enforcement and intelligence services. In that capacity, he regularly responded to requests from the PRC government for information and to terminate video meetings hosted on Company-1’s video communications platform. Part of Jin’s duties included providing information to the PRC government about Company-1’s users and meetings, and in some cases he provided information – such as Internet Protocol addresses, names and email addresses – of users located outside of the PRC. Jin was also responsible for proactively monitoring Company-1’s video communications platform for what the PRC government considers to be “illegal” meetings to discuss political and religious subjects unacceptable to the Chinese Communist Party (CCP) and the PRC government.

As alleged in the complaint, between January 2019 to the present, Jin and others conspired to use Company-1’s systems in the United States to censor the political and religious speech of individuals located in the United States and around the world at the direction and under the control of officials of the PRC government. Among other actions taken at the direction of the PRC government, Jin and others terminated at least four video meetings hosted on Company-1’s networks commemorating the thirty-first anniversary of the Tiananmen Square massacre, most of which were organized and attended by U.S.-based participants, such as dissidents who had participated in and survived the 1989 protests. Some of the participants who were unable to attend these meetings were Company-1 customers in Queens and Long Island, New York who had purchased subscriptions to Company-1’s services, and therefore entered into service agreements with Company-1 governed by its Terms of Service (TOS).

Jin, officials from the PRC government and others allegedly collaborated to identify meeting participants and to disrupt meetings hosted on Company-1’s U.S. servers, at times creating pretextual reasons to justify their actions to other employees and executives of Company-1, as well as Company-1’s users themselves. In particular, in May and June 2020, Jin and others acted to disrupt meetings held on the Company-1 platform to discuss politically sensitive topics unacceptable to the PRC government by infiltrating the meetings to gather evidence about purported misconduct occurring in those meetings. In fact, there was no misconduct; Jin and his co-conspirators fabricated evidence of TOS violations to provide justification for terminating the meetings, as well as certain participants’ accounts. Jin then tasked a high-ranking employee of Company-1 in the United States to effect the termination of meetings and the suspension and cancellation of user accounts.

As detailed in the complaint, Jin’s co-conspirators created fake email accounts and Company-1 accounts in the names of others, including PRC political dissidents, to fabricate evidence that the hosts of and participants in the meetings to commemorate the Tiananmen Square massacre were supporting terrorist organizations, inciting violence or distributing child pornography. The fabricated evidence falsely asserted that the meetings included discussions of child abuse or exploitation, terrorism, racism or incitements to violence, and sometimes included screenshots of the purported participants’ user profiles featuring, for example, a masked person holding a flag resembling that of the Islamic State terrorist group. Jin used the complaints as evidence to persuade Company-1 executives based in the United States to terminate meetings and suspend or terminate the user accounts of the meeting hosts.

PRC authorities took advantage of information provided by Jin to retaliate against and intimidate participants residing in the PRC, or PRC-based family members of meeting participants. PRC authorities temporarily detained at least one person who planned to speak during a commemoration meeting. In another case, PRC authorities visited family members of a participant in the meetings and directed them to tell the participant to cease speaking out against the PRC government and rather to support socialism and the CCP.

The charges in the complaint are allegations, and the defendant is presumed innocent unless and until proven guilty. If convicted of both charged conspiracies, Jin faces a maximum sentence of 10 years in prison.

The investigation into this matter was conducted by the FBI's Washington Field Office. The government's case is being handled by the Office's National Security and Cybercrime Section. Assistant United States Attorneys Alexander A. Solomon, Richard M. Tucker, David K. Kessler and Ian C. Richardson are in charge of the prosecution, with assistance from Trial Attorney Scott A. Claffee of the National Security Division's Counterintelligence and Export Control Section.

The Defendant:

XINJIANG JIN, also known as "Julien Jin"

Age: 39

Zhejiang Province, People's Republic of China

E.D.N.Y. Docket No. 20-MJ-1103

Attachment(s):

[Download Jin Complaint](#)

Topic(s):

Cybercrime

National Security

Component(s):

[USAO - New York, Eastern](#)

Contact:

John Marzulli

United States Attorney's Office

(718) 254-6323

Updated December 18, 2020

EXHIBIT F



An official website of the United States government

[Here's how you know](#)



THE UNITED STATES
DEPARTMENT OF JUSTICE
JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, April 17, 2019

Former Manager for International Airline Pleads Guilty to Acting as an Agent of the Chinese Government

Defendant Placed Packages on Flights from JFK Airport to Beijing at the Direction of Military Officers Assigned to the Chinese Mission to the United Nations

Earlier today, in federal court in Brooklyn, New York, Ying Lin pleaded guilty to acting as an agent of the People's Republic of China (PRC), without notification to the Attorney General, by working at the direction and control of military officers assigned to the Permanent Mission of the People's Republic of China to the United Nations. Lin, a former manager with an international air carrier headquartered in the PRC (the Air Carrier), abused her privileges to transport packages from John F. Kennedy International Airport (JFK Airport) to the PRC aboard Air Carrier flights at the behest of the PRC military officers and in violation of Transportation Security Administration (TSA) regulations. The proceeding was held before United States District Judge Ann M. Donnelly.

Assistant Attorney General for National Security John C. Demers, U.S. Attorney Richard P. Donoghue for the Eastern District of New York, Assistant Director in Charge William F. Sweeney, Jr of the FBI's New York Field Office, and Special Agent in Charge Angel M. Melendez, Department of Homeland Security, Homeland Security Investigations (HSI) announced the guilty plea.

"This case is a stark example of the Chinese government using the employees of Chinese companies doing business here to engage in illegal activity," said Assistant Attorney General Demers. "Covertly doing the Chinese military's bidding on U.S. soil is a crime, and Lin and the Chinese military took advantage of a commercial enterprise to evade legitimate U.S. government oversight."

"The defendant's actions as an agent of the Chinese government helped Chinese military officers to evade U.S. law enforcement scrutiny of packages that they sent from New York to Beijing," stated United States Attorney Donoghue. "This case demonstrates how seriously we address counterintelligence threats posed by individuals in the United States who work for foreign governments, such as China."

"The FBI and our law enforcement partners do all we can every day to protect this country from the threats we can see, and we work even harder to find the threats we can't see," said FBI Assistant Director-in-Charge Sweeney. "Ms. Lin was secreting packages through some of the country's busiest airports, using her work with the Chinese government to thwart our security measures. We believe this case isn't unique and hope it serves as an example that the Chinese and other foreign governments can't break our laws with impunity."

"Lin's criminal actions exploited the international boundary of the United States as she used her position to smuggle packages onto planes headed to China," said HSI Special Agent-in-Charge Melendez. "We are committed to ensuring the integrity of our international airports so they are not used as a front for illicit activities."

Lin worked for the Air Carrier from 2002 through the fall of 2015 as a counter agent at JFK Airport and from the fall of 2015 through April 2016 as the station manager at Newark Liberty International Airport. During her employment with the Air Carrier, Lin accepted packages from the PRC military officers, and placed those packages aboard Air Carrier flights to the PRC as unaccompanied luggage or checked in the packages under the names of other passengers flying on those flights. As the

PRC military officers did not travel on those flights, Lin's actions were contrary to a security program that required that checked baggage be accepted only from ticketed passengers, thereby violating TSA regulations. In addition, Lin encouraged other Air Carrier employees to assist the PRC military officers, instructing those employees that because the Air Carrier was a PRC company, their primary loyalty should be to the PRC.

In exchange for her work at the direction and under the control of PRC military officers and other PRC government officials, Lin received benefits from the PRC Mission and PRC Consulate in New York. These benefits included tax-exempt purchases of liquor, cigarettes and electronic devices worth tens of thousands of dollars. These benefits also included free contracting work at the defendant's two residences in Queens, New York, by PRC construction workers who were permitted under the terms of their visas to work only on PRC government facilities.

When sentenced, Lin faces up to 10 years' imprisonment. As part of the guilty plea, Lin agreed to forfeit approximately \$25,000 as well as an additional \$145,000 in connection with her resolution of the government's forfeiture verdict in United States v. Zhong, No. 16-CR-614 (AMD).

Mr. Demers and Mr. Donoghue expressed their appreciation to the Transportation Security Administration for their assistance on the case. The government's case is being handled by the National Security and Cybercrime Section. Assistant United States Attorneys Douglas M. Pravda, Alexander A. Solomon, Ian C. Richardson and Sarah M. Evans are in charge of the prosecution, with assistance from Trial Attorney Matthew R. Walczewski of the Department of Justice's Counterintelligence and Export Control Section. The forfeiture aspect of the case is being handled by EDNY Assistant United States Attorney Brian Morris of the Office's Civil Division.

Topic(s):

Counterintelligence and Export Control

Component(s):

Federal Bureau of Investigation (FBI).

National Security Division (NSD).

USAO - New York, Eastern

Press Release Number:

19-393

Updated April 17, 2019



THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT *of* NEW YORK

[U.S. Attorneys](#) » [Eastern District of New York](#) » [News](#)

Department of Justice

U.S. Attorney's Office

Eastern District of New York

FOR IMMEDIATE RELEASE

Friday, June 14, 2019

Brooklyn Man Sentenced to 20 Years' Imprisonment for Attempting to Join ISIS in Yemen

Defendant Made Repeated Attempts to Reach ISIS-Controlled Territory and Discussed Plans for a Terror Attack on Times Square Using a Garbage Truck

Earlier today, in federal court in Brooklyn, Mohamed Rafik Naji was sentenced to 20 years' imprisonment by United States District Judge Frederic Block for attempting to provide material support or resources to the Islamic State of Iraq and al-Sham (ISIS), a foreign terrorist organization. Naji pleaded guilty to the charge in February 2018.

Richard P. Donoghue, United States Attorney for the Eastern District of New York, John C. Demers, Assistant Attorney General for National Security, William F. Sweeney, Jr., Assistant Director-in-Charge, Federal Bureau of Investigation, New York Field Office (FBI), and James P. O'Neill, Commissioner, New York City Police Department (NYPD), announced the sentence.

"With today's sentence, Naji has been held accountable for trying to enter a foreign war zone and join ISIS' murderous cause," stated United States Attorney Donoghue. "This Office, together with the FBI, the NYPD and all the members of the FBI Joint Terrorism Task Force will take every step necessary to incapacitate terrorists like Naji and protect the American people. I commend the Task Force for its outstanding work in this case."

"Time and again, the United States has brought to justice those who have traveled from here to try and fight for ISIS," said Assistant Attorney General Demers. "This is just what Naji did. Today's sentence holds him accountable for his crime and I want to thank the agents, analysts, and prosecutors who are responsible for this result."

"Extremists like Mr. Naji believe murdering innocent people advances their political agendas," said FBI Assistant Director-in-Charge Sweeney. "In the end, Mr. Naji, like many others before him, find the only thing their actions lead to is a different vantage point from which to watch the world pass by – through the steel bars of a federal prison. Mr. Naji will remember today as sentencing day, nothing more. Working day in and day out with our partners on the FBI Joint Terrorism Task Force, safeguards have been put in place to secure Times Square and other popular attractions so any would be terrorist will find it extremely difficult to carry out their plans. Our unified goal is to remain proactive and prevent acts before they occur, and once again I would like to thank all of those who ensure our safety."

"This case is a reminder that New York City remains the top target for terrorism in the U.S.," said NYPD Commissioner O'Neill. "The NYPD and its partners in law enforcement will never relent in the fight against terror. I

want to thank the dedicated members of the JTTF who worked on this investigation to keep our City safe and the prosecutors from the Eastern District of New York.”

By late 2014, Naji had become a committed supporter of ISIS as he repeatedly promoted its mission and distributed the terrorist group’s propaganda with violent themes and messages on social media. In March 2015, Naji traveled from New York City to Yemen in an effort to join ISIS. Naji also used social media to advise another person he could travel to join ISIS, but unbeknownst to Naji, that individual was a confidential source of information for the government (the “CS”). In an online conversation with the CS, Naji proclaimed his allegiance to ISIS, stating, “I belong to Islamic state only.”

Following his return to the United States in September 2015, Naji continued to express support for ISIS and violent jihad. In July 2016, following an ISIS-inspired terrorist truck attack in Nice, France that killed scores of civilians, Naji told the CS how easy it would be to carry out a similar attack in Times Square: “[ISIS] want an operation in Times Square” and “[an ISIS] reconnaissance group . . . put up scenes of Times Square.” Naji added: “if there is a truck, I mean a garbage truck and one drives it there to Times Square and crushes them . . . Times Square day.”

Naji has been incarcerated since his arrest in Brooklyn in November 2016.

The government’s case is being handled by the Office’s National Security and Cybercrime Section. Assistant United States Attorney Ian C. Richardson is in charge of the prosecution, with assistance from Trial Attorney Jacqueline L. Barkett of the National Security Division’s Counterterrorism Section.

The Defendant:

MOHAMED RAFIK NAJI

Age: 40

Brooklyn, New York

E.D.N.Y. Docket No. 16-CR-653 (FB)

Topic(s):

Counterterrorism

Component(s):

Federal Bureau of Investigation (FBI)

National Security Division (NSD)

USAO - New York, Eastern

Contact:

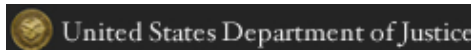
John Marzulli

Tyler Daniels

United States Attorney’s Office

(718) 254-6323

Updated June 14, 2019



THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT *of* NEW YORK

[U.S. Attorneys](#) » [Eastern District of New York](#) » [News](#)

Department of Justice

U.S. Attorney's Office

Eastern District of New York

FOR IMMEDIATE RELEASE

Thursday, November 7, 2019

**Aventura Technologies, Inc. and its Senior Management Charged
with Fraud, Money Laundering and Illegal Importation of
Equipment Manufactured in China**

**The Long Island Company Supplied Chinese-Made Surveillance Equipment to U.S.
Government and Private Customers While Falsely Claiming its Products Were “Made in
U.S.A.”**

A criminal complaint was unsealed today in federal court in Brooklyn charging surveillance and security equipment company Aventura Technologies, Inc. (Aventura), located in Commack, New York, and seven current and former employees with selling Chinese-made equipment with known cybersecurity vulnerability to government and private customers while falsely representing that the equipment was made in the United States and concealing that the products were manufactured in the People's Republic of China (PRC). Aventura has generated more than \$88 million in sales revenue since November 2010, and the charged scheme has been ongoing since 2006.

In addition to Aventura, the individual defendants charged in the complaint are Jack Cabasso, Aventura's Managing Director and de facto owner and operator; Frances Cabasso, his wife and Aventura's purported owner and Chief Executive Officer; senior executives Jonathan Lasker, Christine Lavonne Lazarus and Eduard Matulik; current employee Wayne Marino; and recently retired employee Alan Schwartz.

Four of the individual defendants are also charged with defrauding the U.S. government by falsely claiming that Frances Cabasso was the owner and operator of the company in order to obtain access to valuable government contracts reserved for women-owned businesses when, in fact, Aventura was actually controlled by her husband, Jack Cabasso. The Cabassos are also charged with laundering the monetary proceeds of these fraudulent schemes.

Six of the defendants were arrested this morning and are scheduled to be arraigned this afternoon before United States Magistrate Judge Ramon E. Reyes, Jr. Law enforcement agents executed search warrants at Aventura's headquarters in Commack, New York, and at the home of Jack and Frances Cabasso in Northport, New York. The government has also seized the Cabassos' 70-foot luxury yacht, and has frozen approximately \$3 million in 12 financial accounts that contain proceeds from the defendants' unlawful conduct.

Richard P. Donoghue, United States Attorney for the Eastern District of New York; William F. Sweeney, Jr., Assistant Director-in-Charge, Federal Bureau of Investigation, New York Field Office (FBI); Joseph P. Dattoria, Special Agent-in-Charge, U.S. General Services Administration, Office of Inspector General (GSA-OIG); Leigh-Alistair Barzey, Special Agent-in-Charge, Defense Criminal Investigative Service, Northeast Field Office (DCIS); J.

Russell George, Treasury Inspector General for Tax Administration (TIGTA); Troy Miller, Director of Field Operations, U.S. Customs and Border Protection, New York Field Office (CBP); Jonathan D. Larsen, Special Agent-in-Charge, Internal Revenue Service, Criminal Investigation, New York (IRS-CI); Jason T. Hein, Special Agent-in-Charge, U.S. Air Force Office of Special Investigations, Office of Procurement Fraud Investigations, Detachment Six (AFOSI); Leo Lamont, Special Agent-in-Charge, Naval Criminal Investigative Service (NCIS); and Teri L. Donaldson, Inspector General, U.S. Department of Energy, Office of Inspector General (DOE-OIG), announced the charges.

"As alleged, the defendants falsely claimed for years that their surveillance and security equipment was manufactured on Long Island, padding their pockets with money from lucrative contracts without regard for the risk to our country's national security posed by secretly peddling made-in-China electronics with known cyber vulnerabilities," stated United States Attorney Donoghue. "With today's arrests, the defendants' brazen deceptions and fraud schemes have been exposed, and they will face serious consequences for slapping phony 'Made in the U.S.A.' labels on products that our armed forces and other sensitive government facilities depended upon." Mr. Donoghue expressed his appreciation to U.S. Army Criminal Investigation Command's Major Procurement Fraud Unit for their work on the case.

"Greed is at the heart of this scheme, a reprehensible motive when the subjects in this case allegedly put into question the security of men and women who don uniforms each day to protect our nation," stated FBI Assistant Director-in-Charge Sweeney. "There is no mistaking the cyber vulnerabilities created when this company sold electronic surveillance products made in the PRC, and then using those items in our government agencies and the branches of our armed forces. I cannot stress enough that we will do everything we can to search out and stop any other company willing to cut corners and pocket profits that endanger the lives of Americans, and make this country less safe."

"The laws in place regulating government contracts ensure both the taxpayer and government receive quality goods and services at competitive prices. In addition, they provide a fair opportunity and level playing field for all businesses seeking government contracts. The General Services Administration's Office of Inspector General will continue to work closely with our law enforcement partners to aggressively investigate allegations of fraud against the United States Government," stated GSA-OIG Special Agent-in-Charge Dattoria.

"The arrests and other enforcement operations that occurred today were the direct result of a joint investigative effort," stated DCIS Special Agent-in-Charge Barzey. "The introduction of counterfeit parts and materials into the U.S. Defense Department's supply chain poses a significant risk and impacts America's military readiness and our national security. The DCIS is committed to working with its law enforcement partners and the U.S. Attorney's Office, Eastern District of New York, to ensure that individuals and companies who engage in fraudulent activity, at the expense of the U.S. military, are investigated and prosecuted."

"TIGTA's mission includes investigating allegations of waste, fraud or abuse involving the Internal Revenue Service (IRS)," stated TIGTA Inspector General George. "Mr. Cabasso and his co-conspirators secured products from outside of the U.S. while purporting that these products were made in America. They then sold these products to the U.S. Government, including the IRS and other Government agencies. TIGTA is committed to investigating and working with our law enforcement partners to root out this type of fraud from the Government contracting and procurement process. I want to thank U.S. Attorney Donoghue for the steadfast support that he and his talented prosecutors gave to this investigation."

"U.S. Customs and Border Protection provided the critical link to an ongoing investigation that resulted in the takedown of an elaborate criminal enterprise," stated CBP Director of Field Operations Miller. "This case serves as a great example of collaborative law enforcement efforts to uncover and dismantle criminal enterprises that seek to defraud the United States government for personal gain while jeopardizing our national defense and causing economic harm to their competitors."

"In today's global economy, 'Made in the USA' is too sacred of a mark to fraudulently use for one's self interest," stated IRS-CI Special Agent-in-Charge Larsen. "IRS-Criminal Investigation works diligently with our law

enforcement partners to uncover con artists devising elaborate schemes to become independently wealthy. These allegations have serious national security implications that go beyond shameless attempts at personal enrichment.”

“Product substitution is a serious crime that puts our men and women in uniform at greater risk,” stated NCIS Special Agent-in-Charge Lamont. “Our Sailors, Marines, and other armed services personnel deserve to have equipment that meets the highest standards for safety and performance, which will not fail them when it matters most. Substandard and counterfeit parts simply cannot be depended upon. Investigating product substitution and mitigating risks to the Department of the Navy supply chain is a top priority for the Naval Criminal Investigative Service. NCIS has a cadre of Special Agents trained in all aspects of economic crime, tirelessly fighting fraud in the procurement process.”

“Ensuring the integrity of the US Air Force procurement process and the quality of the products provided to our warfighters is a top investigative priority of the Air Force Office of Special Investigations,” stated AFOSI Special Agent-in-Charge Hein. “Those who seek to conduct business with the Air Force must be candid and truthful. AFOSI will aggressively investigate those who attempt to defraud the Air Force, and will work with our law enforcement partners to identify and prosecute those who would take advantage of the USAF and its interests. The victims are not just our men and women in uniform, but every American taxpayer.”

“The Department of Energy’s Office of Inspector General remains committed to ensuring the integrity and security of the Department’s vendors, especially given the serious nature of the Department’s mission,” stated DOE Inspector General Donaldson. “We take allegations of conspiracy against the U.S. Government very seriously and will aggressively investigate these matters to protect the Department and the American taxpayers. We appreciate the collaborative efforts of the DOJ and our other law enforcement partners.”

The Country of Origin Fraud and Unlawful Importation Scheme

As charged in the criminal complaint and in court documents filed today,[1] for over a decade Aventura lied to its customers, including the U.S. military, the federal government and private customers in the United States and abroad. Under federal government procurement laws and regulations a product’s country of origin can impact a procurement officer’s decision to purchase a product. A product’s country of origin also matters to some private sector customers. In addition, all products imported into the United States must be marked with their country of origin. Over the past decade, Aventura made upwards of \$88 million, including over \$20 million in federal government contracts, while claiming that it was manufacturing its products at its headquarters in Commack. In fact, Aventura does not manufacture anything in the United States. Instead, since at least 2006, Aventura has been importing products primarily from the PRC, then reselling them as American-made or manufactured in a small number of other countries.

Notably, Aventura imported networked security products from PRC manufacturers with known cybersecurity vulnerabilities, and resold them to U.S. military and other government installations while claiming that they were American-made. Aventura similarly deceived private customers in the United States and abroad who paid a premium for what they believed to be American-made goods. As a result, Aventura not only defrauded its customers, but also exposed them to serious, known cybersecurity risks, and created a channel by which hostile foreign governments could have accessed some of the government’s most sensitive facilities.

For this conduct, Aventura and the seven individual defendants are charged with unlawful importation and conspiracy to commit wire and bank fraud.

In the course of its investigation, the government intercepted and covertly marked numerous shipments from PRC sources to Aventura’s Commack headquarters. In some cases, cameras shipped from the PRC were pre-marked with Aventura’s logo and the phrase “Made in USA,” accompanied by an American flag. In many instances, the items were later resold to government agencies to whom the defendants falsely represented that the products were American-made.

For example, in March 2019 the U.S. Navy ordered from Aventura a \$13,500 laser-enhanced night vision camera that was specified as American-made on Aventura's U.S. General Services Administration (GSA) price list. (In fact, no item on Aventura's GSA price list is listed as being made in the PRC.) In April 2019, at a shipping facility in Jamaica, Queens, a team led by CBP officers intercepted a shipment from a PRC manufacturer ("PRC Manufacturer-3") to Aventura that contained a camera matching the Navy's order and surreptitiously marked it for later identification using a method that would not be apparent to a casual observer.^[2] Two weeks later, that same camera was delivered to Naval Submarine Base New London in Groton, Connecticut.

In another instance, in September 2018, the Department of Energy (DOE) ordered approximately \$156,000 worth of networked automated turnstiles from Aventura, to be installed at a facility in Tennessee. Aventura's GSA price list described the turnstiles as American-made. In January 2019, turnstiles matching DOE's order were intercepted in a shipment from a PRC manufacturer and marked by CBP; one month later, they arrived at the DOE facility in Tennessee. The crates shipped by Aventura to the DOE appeared identical to those that the CBP-led team had inspected, except that the shipping labels from the PRC directing the crates to Aventura had been peeled off, leaving behind visible traces of paper and glue. A special agent with the DOE-OIG placed a call to Lazarus regarding the turnstile shipment in May 2015. During the call, Lazarus falsely stated that the turnstiles were "U.S. made [in] New York."

As a third example, in 2018, Aventura sold the U.S. Air Force 25 body cameras for use by Air Force security personnel at an Air Force base. Aventura was contractually required to provide goods from a limited set of countries that did not include the PRC. In August 2018, however, an Air Force service member observed Chinese characters on the built-in screen of one of the body cameras. The body camera was sent for analysis to a specialist, who downloaded its firmware and found numerous indications that the camera was manufactured in PRC. The camera contained multiple preloaded images that were apparently designed to display on the built-in screen—including the U.S. Air Force logo, the logo of the PRC Ministry of Public Security and the logo of PRC Manufacturer-1. All three logos had been saved to the camera's firmware using the same software, on a computer that was set to a time zone in the PRC—indicating that the camera's manufacturer in the PRC had been aware that the U.S. Air Force was a likely end user of the camera.

The defendants, working with counterparts in the PRC, took extraordinary steps to conceal this scheme. In November 2018, Jack Cabasso exchanged emails with an employee of a PRC manufacturer of surveillance equipment (PRC Manufacturer-2), identifying the need to "hide" the name of PRC Manufacturer-2 from Aventura's customers. Cabasso wrote that Schwartz was "putting together a list" of steps to be taken. One week later, Cabasso stressed the need to take steps so that "they cannot trace" the product to PRC Manufacturer-2, adding, "The housings are a problem since you publish them on your website but nothing we can do about that." Cabasso added that "the biggest problem" was that PRC Manufacturer-2's initials were marked on its circuit boards, and said that he had "lost several potential customers" because of similar practices by another PRC manufacturer (PRC Manufacturer-1). The employee responded that the company's initials would be removed from all circuit boards shipped to Aventura. Lasker was copied on all of the emails in this sequence.

Similarly, in December 2018, Jack Cabasso and Marino exchanged emails with employees of another PRC-based digital video equipment manufacturer (PRC Manufacturer-4). Marino complained to the employees that "communication from the server to the client contains [PRC Manufacturer-4's name] visible in clear text. This should be changed." When one of the employees wrote that this could not be changed, Cabasso responded: "WE CANNOT HAVE CUSTOMERS ABLE TO SEE" PRC Manufacturer-4's name, later adding, "we also sent a sample to a customer and he found [PRC Manufacturer-4]. . . branding in the [operating system] which is a problem." Schwartz and Lasker, among others, were included on these communications.

On or about November 23, 2016, Jack Cabasso sent an email to a GSA representative accusing 12 other GSA contractors of selling products to the U.S. Government that were manufactured by a PRC manufacturer of surveillance equipment (PRC Manufacturer-1). Cabasso asserted that this was a "big problem" and "doesn't get any worse," because PRC Manufacturer-1 was "actually the Communist Chinese Government and ha[d] 'significant' cybersecurity issues aside from" compliance with U.S. laws specifying country-of-origin requirements for government purchases. Cabasso stated that PRC Manufacturer-1 "will acknowledge they manufacture no

products outside of China,” and appended an article about the removal of cameras manufactured by PRC Manufacturer-1 from the U.S. Embassy in Afghanistan.

Notably, Aventura was importing security equipment from PRC Manufacturer-1 while Jack Cabasso was complaining to GSA about other contractors’ supposed dealings with the company. For example, bank records show that Aventura wired funds to PRC Manufacturer-1 in the PRC on or about October 31, 2016 and November 29, 2016. And, law enforcement records show that on or about December 13, 2016, Aventura imported from PRC Manufacturer-1 in PRC an approximately 1,800-pound shipment of goods manifested as “digital video.”

In November 2018, Jack Cabasso and Matulik communicated with a potential distributor in Qatar, who asked for assurance that Aventura’s cameras were American made. Cabasso responded: “I believe Ed confirmed that they are made in the Aventura factory here in New York and [anyone] may visit at any time.” Cabasso attached what purported to be a photograph of Aventura’s assembly line, depicting a row of seated individuals in blue lab coats and protective hairnets working at laboratory benches—a photograph that also appears on Aventura’s website. In reality, this photograph first appeared in a trade publication article recounting a reporter’s visit to PRC Manufacturer-1’s manufacturing facility in Hangzhou, PRC, and it depicts PRC Manufacturer-1’s assembly line, not Aventura’s.

The Scheme to Misrepresent Aventura as a Woman-Owned Small Business

Jack and Frances Cabasso, along with Lasker and Lazarus, falsely represented on numerous occasions that Frances Cabasso was the chief executive of Aventura. In fact, the true chief executive officer of Aventura was Jack Cabasso, and Frances Cabasso played a minimal role at the company. This misrepresentation gave Aventura access to government contracts that were set aside for women-owned small businesses, a category that is legally defined to include only those businesses owned by women, where management and daily operations are also controlled by one or more women.

In order to win these set-asides, the defendants represented to the public that Frances Cabasso controlled Aventura. Aventura’s website and its GSA webpage identify Aventura as a woman-owned business, and the defendants repeatedly certified to the GSA and stated to government procurement officers that Aventura is a woman-owned business. For example, on or about January 13, 2014, a GSA employee emailed Frances Cabasso to “verify if Aventura Technologies, Inc. is a Woman-Owned business.” She replied: “Yes we are still a certified women-owned business.” Aventura has won numerous contracts from the federal government on the strength of its status as a woman-owned business.

As Jack Cabasso repeatedly admitted, he was the true chief executive officer of Aventura. In 2017, Jack Cabasso emailed an Air Force procurement officer, stating in part, “I am the Managing Director of Aventura Technologies and the senior most person within the organization.” Similarly, in a 2018 deposition, Cabasso said that his job responsibilities were to “oversee all operations of the company.” By contrast, Frances Cabasso has worked as a bookkeeper at an unrelated accounting firm since 2011 and is rarely present at Aventura’s offices. At times, emails sent to Frances Cabasso’s email address appear to have been auto-forwarded to Jack Cabasso who sometimes signed his responses in Frances’s name. The defendants joked about the fact that Frances Cabasso did not work at Aventura. For example, in an instant message exchange on December 5, 2016 between Jack Cabasso and Lazarus, both defendants discussed moving another employee into “Fran’s” office—the office of the purported owner of the company—putting the name “Fran’s” in quotation marks.

The Money Laundering Scheme

Jack and Frances Cabasso siphoned Aventura’s illegal profits out of the company through a network of shell companies and intermediaries. The funds were then directed to investments owned by the Cabassos or controlled for their benefit.

Between 2016 and 2018, Aventura transferred approximately \$2 million to an attorney escrow account belonging to a Long Island, New York-based law firm (Law Firm-1), some of which appears to have been intended to conceal the source of the funds. For example, on or about May 24, 2016, Aventura transferred \$450,000 to Law Firm-1.

On the same day, Law Firm-1 paid a total of \$435,000 towards the purchase of a new home for a relative of Jack and Frances Cabasso.

Similarly, in early 2018, Aventura transferred \$675,000 to Law Firm-1. Those funds were loaned out to a separate company for use in purchasing a house. When that company repaid the loan to Law Firm-1, the proceeds, totaling approximately \$682,000, were transferred to Frances Cabasso.

In addition to the transactions through Law Firm-1, Aventura has transferred at least \$2.75 million to shell companies owned by Frances Cabasso. Those funds were then transferred to a number of accounts, including Frances Cabasso's personal bank account and the business account of a lawyer retained by Jack Cabasso. Some of these funds were returned to Aventura's bank accounts, in transactions having no discernible economic purpose.

In addition to these and other transfers, Aventura has made approximately \$1 million in payments since 2013 related to the Cabassos' 70-foot luxury yacht, known as the *Tranquilo*, which is moored in the gated community where the Cabassos reside. Although Aventura is the purported owner of the *Tranquilo*, the yacht appears to have no connection with Aventura's corporate business, and its rental income flows to the Cabassos, not to Aventura.

The defendants are presumed innocent unless and until proven guilty. If convicted, the defendants each face up to 20 years' imprisonment on each charge in the complaint.

The government's case is being handled by the Office's National Security and Cybercrime Section. Assistant United States Attorneys Ian C. Richardson, Alexander Mindlin, Kayla Bensing and Claire Kedeshian are in charge of the prosecution.

The FBI has established an email hotline for potential victims. If you have information regarding Aventura's crimes or believe that you may be a victim, please send an email to NY-AventuraVictims@fbi.gov

The Defendants:

AVENTURA TECHNOLOGIES, INC.
Commack, New York

FRANCES CABASSO
Age: 59
Northport, New York

JACK CABASSO
Age: 61
Northport, New York

JONATHAN LASKER
Age: 34
Port Jefferson Station, New York

CHRISTINE LAVONNE LAZARUS
Age: 45
Shirley, New York

WAYNE MARINO
Age: 39
Rocky Point, New York

EDUARD MATULIK

Age: 42

North Massapequa, New York

ALAN SCHWARTZ

Age: 70

Smithtown, New York

E.D.N.Y. Docket No. 19-MJ-1035

[1] As the introductory phrase signifies, the entirety of the text of the complaint and the description of the complaint set forth herein, constitute only allegations and every fact described should be treated as an allegation.

[2] The numerals used to identify the manufacturers in this press release correspond to the way they are referred to in the criminal complaint.

Attachment(s):

[Download Aventura et al Complaint](#)

Topic(s):

Cybercrime

Financial Fraud

National Security

Component(s):

[USAO - New York, Eastern](#)

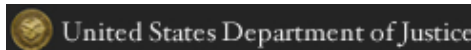
Contact:

John Marzulli

United States Attorney's Office

(718) 254-6323

Updated November 7, 2019



THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT *of* NEW YORK

[U.S. Attorneys](#) » [Eastern District of New York](#) » [News](#)

Department of Justice

U.S. Attorney's Office

Eastern District of New York

FOR IMMEDIATE RELEASE

Monday, November 25, 2019

Former Chinese Diplomat and Head of U.S. Operations for Chinese Construction Business Sentenced to 190 Months' Imprisonment for Engaging in Forced Labor and Related Charges

Earlier today, in federal court in Brooklyn, Dan Zhong, a former diplomat of the People's Republic of China (PRC), was sentenced by United States District Judge Ann M. Donnelly to 190 months' imprisonment and a \$50,000 fine. Zhong, the former head of U.S. operations of Chinese Liaoning Rilin Construction (Group) Co. Ltd. (also known as China Rilin) and U.S.-based subsidiaries, including U.S. Rilin, was convicted by a federal jury in March 2019 following a three-week trial on charges of conspiracy to provide forced labor, providing and benefitting from forced labor, concealing passports and immigration documents in connection with forced labor, conspiracy to commit alien smuggling and conspiracy to commit visa fraud. The Court also ordered Zhong to forfeit his interests in multiple real estate properties and pay approximately \$23,000 in restitution as part of the sentence.

Richard P. Donoghue, United States Attorney for the Eastern District of New York, William F. Sweeney, Jr., Assistant Director-in-Charge, Federal Bureau of Investigation, New York Field Office (FBI), Peter C. Fitzhugh, Special Agent-in-Charge, Department of Homeland Security, Homeland Security Investigations, New York (HSI), and Timothy W. Dumas, Special Agent-in-Charge, U.S. Department of State's Diplomatic Security Service, New York Field Office (DSS), announced the sentence.

"Unlike Chinese Communist elites, Americans do not practice, condone or tolerate forced labor," stated United States Attorney Donoghue. "Mr. Zhong, a former long-time PRC diplomat, oppressed and coerced Chinese construction workers in New York, forcing some to work for years without pay under the threat of physical harm and financial ruin. Zhong will now pay a heavy price for those crimes." Mr. Donoghue expressed his appreciation to the Department of State's Office of Foreign Missions and the FBI's Field Office in Newark, New Jersey, for their assistance on the case.

"Zhong forced his workers to work 14-hour days and live in cramped, unsafe conditions, with locks on the doors so they could not escape," stated HSI Special Agent-in-Charge Fitzhugh. "Through forced labor, Zhong took advantage of those seeking a new life in America. Today's sentencing is a testament to law enforcement's resolve to arrest and prosecute anyone seeking to exploit people for person gain."

"The Diplomatic Security Service works to identify and prevent situations where vulnerable individuals are exploited in human trafficking schemes such as this," stated DSS Special Agent-in-Charge Dumas. "This case is an especially serious abuse of the legal and immigration systems as it involved a former diplomat of the People's Republic of China. DSS agents stationed throughout the world are well-positioned to work with U.S. and foreign

partners to stop those individuals who would manipulate instruments of international travel, and profit from the selling of human beings.”

Zhong’s company performed construction work on a variety of PRC government facilities in the United States, including the Permanent Mission of the PRC to the United Nations, the Embassy of the PRC to the United States and PRC Consulates General in the United States. Zhong and his co-conspirators obtained visas for PRC workers that required them to work only at PRC diplomatic facilities. In fact, they were forced to work on private construction projects, including a commercial building in midtown Manhattan, and private residences in Queens and on Long Island. Zhong also used the workers as personal servants – preparing meals, chauffeuring him and performing yard work at his home.

Zhong and his co-conspirators required PRC workers to turn over substantial “security deposits,” including the deeds to their family homes that were subject to forfeiture if they refused to work, as a key element of the “debt bondage” contracts the workers signed. Once in the United States, the workers were forced to surrender their passports to Zhong’s co-conspirators. The workers were required to work 14-hour days, seven days a week, for years without receiving any pay. Twenty or more workers were housed in one and two-family houses in Jersey City. Inspections of these houses revealed numerous fire code violations, as well as illegal locks to prevent the workers from escaping. Zhong and his co-conspirators resorted to physical force and threats to prevent escape by the workers, including forcing the workers’ family members out of their homes in the PRC. Zhong’s co-defendant in the indictment, Landong Wang, is a fugitive who is believed to be in the PRC.

The government’s case is being handled by the Office’s National Security and Cybercrime Section. Assistant United States Attorneys Alexander A. Solomon, Douglas M. Pravda, Ian C. Richardson and Craig R. Heeren are in charge of the prosecution, with assistance provided by Assistant United States Attorney Brian Morris of the Office’s Civil Division which is handling the forfeiture aspect of the case.

The Defendant:

DAN ZHONG

Age: 49

Livingston, New Jersey

E.D.N.Y. Docket No. 16-CR-614 (AMD)

Topic(s):

Immigration

Component(s):

USAO - New York, Eastern

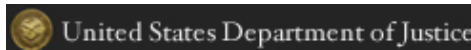
Contact:

John Marzulli

United States Attorney’s Office

(718) 254-6323

Updated November 25, 2019



THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT *of* NEW YORK

[U.S. Attorneys](#) » [Eastern District of New York](#) » [News](#)

Department of Justice

U.S. Attorney's Office

Eastern District of New York

FOR IMMEDIATE RELEASE

Sunday, May 31, 2020

Two Brooklyn Residents and a Greene County Resident Charged in Connection with Molotov Cocktail Attacks on the NYPD

Two criminal Complaints were filed Saturday evening in federal court in Brooklyn charging two women and a man with using and attempting to use improvised incendiary devices commonly known as "Molotov Cocktails" to damage and destroy New York City Police Department (NYPD) vehicles. Defendants Colinford Mattis and Urooj Rahman, both residents of Brooklyn, were arrested in a van early Saturday morning while allegedly in possession of explosive device components shortly after Rahman hurled a Molotov cocktail at an NYPD vehicle before fleeing with Mattis. A separate complaint charges Samantha Shader, a resident of Catskill, New York, who was arrested after allegedly throwing a Molotov cocktail at an NYPD vehicle occupied by four police officers. The defendants charged in each of the complaints will make their initial appearances via teleconference on Monday, June 1, 2020, before United States Magistrate Judge Steven M. Gold.

Richard P. Donoghue, United States Attorney for the Eastern District of New York, William F. Sweeney, Jr., Assistant Director-in-Charge, Federal Bureau of Investigation, New York Field Office (FBI), and Dermot F. Shea, Commissioner, NYPD, announced the arrests and charges.

"These defendants are charged with attacking the New York City Police Department while its Police Officers are risking their lives to protect the Constitutional rights of protesters and the safety of us all," stated United States Attorney Donoghue. "No rational human being can ever believe that hurling firebombs at Police Officers and vehicles is justified. The Eastern District of New York will do everything in its power to protect those who protect us all, and we will ensure that criminals who use the camouflage of lawful protest to launch violent attacks against Police Officers face justice."

"When you conduct a violent attack that breaks federal law, the FBI New York office, along with our NYPD and Department of Justice partners, will move with speed to hold you accountable. Behavior like the attacks charged here puts our entire community - protestors and first responders alike - in danger, and we will simply not allow it to go unaddressed. The consequences for conducting this alleged attack, and any similar activity planned for the future, will be severe," stated FBI Assistant Director-in-Charge Sweeney.

"Molotov Cocktails are violent tools of individuals looking to inflict harm and damage our city. Crimes like these are devastating to their targets and also to the protestors and their right to free speech that police are working hard to protect. It is reassuring that the U.S. Attorney in Brooklyn has taken this case. I'm confident that the severest penalties under the law will be sought," stated NYPD Commissioner Shea.

As detailed in the complaint charging Mattis and Rahman, an NYPD surveillance camera recorded Rahman tossing a Molotov Cocktail at an unoccupied NYPD vehicle parked near the 88th Precinct in Brooklyn, New York and then fleeing in a tan minivan. Officers pursued the minivan and arrested Rahman and Mattis, who was the vehicle's driver. The NYPD recovered several precursor items used to build Molotov Cocktails, including a lighter, a bottle filled with toilet paper and a liquid suspected to be gasoline in the vicinity of the passenger seat and a gasoline tank in the rear of the vehicle.

As detailed in the complaint charging Shader, a video recorded by a witness captured her igniting a Molotov Cocktail and throwing it at an NYPD vehicle occupied by four police officers, shattering two of its windows. Police officers pursued Shader as she attempted to flee and apprehended her. In a post-arrest statement, Shader later admitted to police that she had thrown the Molotov Cocktail at the NYPD vehicle.

The charges in the Complaints are allegations, and the defendants are presumed innocent unless and until proven guilty. If convicted, each defendant faces a mandatory-minimum sentence of 5 years and up to 20 years' imprisonment.

The government's case is being handled by the Office's National Security and Cybercrime Section. Assistant United States Attorneys Ian C. Richardson and Jonathan Algor are in charge of the prosecution.

The Defendants:

COLINFORD MATTIS

Age: 32

Brooklyn, New York

UROOJ RAHMAN

Age: 31

Brooklyn, New York

E.D.N.Y. Docket No. 20-MJ-403

SAMANTHA SHADER

Age: 27

Catskill, New York

E.D.N.Y. Docket No. 20-MJ-402

Attachment(s):

[Download Mattis and Rahman Complaint](#)

[Download Shader Complaint](#)

Topic(s):

Violent Crime

Component(s):

[USAO - New York, Eastern](#)

Contact:

John Marzulli

United States Attorney's Office

(718) 254-6323



THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT *of* NEW YORK

[U.S. Attorneys](#) » [Eastern District of New York](#) » [News](#)

Department of Justice

U.S. Attorney's Office

Eastern District of New York

FOR IMMEDIATE RELEASE

Friday, December 18, 2020

**China-Based Executive at U.S. Telecommunications Company
Charged with Disrupting Video Meetings Commemorating
Tiananmen Square Massacre**

**Defendant Coordinated with the PRC Government to Target Dissidents and Disrupt
Meetings**

A complaint and arrest warrant were unsealed today in federal court in Brooklyn charging Xinjiang Jin, also known as "Julien Jin," with conspiracy to commit interstate harassment and unlawful conspiracy to transfer a means of identification. Jin, an employee of a U.S.-based telecommunications company (Company-1) who was based in the People's Republic of China (PRC), allegedly participated in a scheme to disrupt a series of meetings in May and June 2020 held to commemorate the June 4, 1989 Tiananmen Square massacre in the PRC. The meetings were conducted using a videoconferencing program provided by Company-1, and were organized and hosted by U.S.-based individuals, including individuals residing in the Eastern District of New York. Jin is not in U.S. custody.

Seth D. DuCharme, Acting United States Attorney for the Eastern District of New York; John C. Demers, Assistant Attorney General for National Security; and Christopher Wray, Director, Federal Bureau of Investigation (FBI), announced the charges.

"The allegations in the complaint lay bare the Faustian bargain that the PRC government demands of U.S. technology companies doing business within the PRC's borders, and the insider threat that those companies face from their own employees in the PRC," stated Acting United States Attorney DuCharme. "As alleged, Jin worked closely with the PRC government and members of PRC intelligence services to help the PRC government silence the political and religious speech of users of the platform of a U.S. technology company. Jin willingly committed crimes, and sought to mislead others at the company, to help PRC authorities censor and punish U.S. users' core political speech merely for exercising their rights to free expression. The charges announced today make clear that employees working in the PRC for U.S. technology companies make those companies—and their users—vulnerable to the malign influence of the PRC government. This Office will continue working tirelessly to protect against threats to the free expression of political views and religious beliefs, regardless whether those threats come from inside or outside the United States." Mr. DuCharme and Mr. Demers also extended their thanks and appreciation to Company-1 for its cooperation in the government's ongoing investigation.

"No company with significant business interests in China is immune from the coercive power of the Chinese Communist Party," stated Assistant Attorney General Demers. "The Chinese Communist Party will use those within its reach to sap the tree of liberty, stifling free speech in China, the United States and elsewhere about the Party's repression of the Chinese people. For companies with operations in China, like that here, this reality may

mean executives being coopted to further repressive activity at odds with the values that have allowed that company to flourish here.”

“The FBI remains committed to protecting the exercise of free speech for all Americans. As this complaint alleges, that freedom was directly infringed upon by the pernicious activities of Communist China’s Intelligence Services, in support of a regime that neither reflects nor upholds our democratic values,” stated FBI Director Wray. “Americans should understand that the Chinese Government will not hesitate to exploit companies operating in China to further their international agenda, including repression of free speech.”

According to the complaint, Jin served as Company-1’s primary liaison with PRC law enforcement and intelligence services. In that capacity, he regularly responded to requests from the PRC government for information and to terminate video meetings hosted on Company-1’s video communications platform. Part of Jin’s duties included providing information to the PRC government about Company-1’s users and meetings, and in some cases he provided information – such as Internet Protocol addresses, names and email addresses – of users located outside of the PRC. Jin was also responsible for proactively monitoring Company-1’s video communications platform for what the PRC government considers to be “illegal” meetings to discuss political and religious subjects unacceptable to the Chinese Communist Party (CCP) and the PRC government.

As alleged in the complaint, between January 2019 to the present, Jin and others conspired to use Company-1’s systems in the United States to censor the political and religious speech of individuals located in the United States and around the world at the direction and under the control of officials of the PRC government. Among other actions taken at the direction of the PRC government, Jin and others terminated at least four video meetings hosted on Company-1’s networks commemorating the thirty-first anniversary of the Tiananmen Square massacre, most of which were organized and attended by U.S.-based participants, such as dissidents who had participated in and survived the 1989 protests. Some of the participants who were unable to attend these meetings were Company-1 customers in Queens and Long Island, New York who had purchased subscriptions to Company-1’s services, and therefore entered into service agreements with Company-1 governed by its Terms of Service (TOS).

Jin, officials from the PRC government and others allegedly collaborated to identify meeting participants and to disrupt meetings hosted on Company-1’s U.S. servers, at times creating pretextual reasons to justify their actions to other employees and executives of Company-1, as well as Company-1’s users themselves. In particular, in May and June 2020, Jin and others acted to disrupt meetings held on the Company-1 platform to discuss politically sensitive topics unacceptable to the PRC government by infiltrating the meetings to gather evidence about purported misconduct occurring in those meetings. In fact, there was no misconduct; Jin and his co-conspirators fabricated evidence of TOS violations to provide justification for terminating the meetings, as well as certain participants’ accounts. Jin then tasked a high-ranking employee of Company-1 in the United States to effect the termination of meetings and the suspension and cancellation of user accounts.

As detailed in the complaint, Jin’s co-conspirators created fake email accounts and Company-1 accounts in the names of others, including PRC political dissidents, to fabricate evidence that the hosts of and participants in the meetings to commemorate the Tiananmen Square massacre were supporting terrorist organizations, inciting violence or distributing child pornography. The fabricated evidence falsely asserted that the meetings included discussions of child abuse or exploitation, terrorism, racism or incitements to violence, and sometimes included screenshots of the purported participants’ user profiles featuring, for example, a masked person holding a flag resembling that of the Islamic State terrorist group. Jin used the complaints as evidence to persuade Company-1 executives based in the United States to terminate meetings and suspend or terminate the user accounts of the meeting hosts.

PRC authorities took advantage of information provided by Jin to retaliate against and intimidate participants residing in the PRC, or PRC-based family members of meeting participants. PRC authorities temporarily detained at least one person who planned to speak during a commemoration meeting. In another case, PRC authorities visited family members of a participant in the meetings and directed them to tell the participant to cease speaking out against the PRC government and rather to support socialism and the CCP.

The charges in the complaint are allegations, and the defendant is presumed innocent unless and until proven guilty. If convicted of both charged conspiracies, Jin faces a maximum sentence of 10 years in prison.

The investigation into this matter was conducted by the FBI's Washington Field Office. The government's case is being handled by the Office's National Security and Cybercrime Section. Assistant United States Attorneys Alexander A. Solomon, Richard M. Tucker, David K. Kessler and Ian C. Richardson are in charge of the prosecution, with assistance from Trial Attorney Scott A. Claffee of the National Security Division's Counterintelligence and Export Control Section.

The Defendant:

XINJIANG JIN, also known as "Julien Jin"

Age: 39

Zhejiang Province, People's Republic of China

E.D.N.Y. Docket No. 20-MJ-1103

Attachment(s):

[Download Jin Complaint](#)

Topic(s):

Cybercrime

National Security

Component(s):

[USAO - New York, Eastern](#)

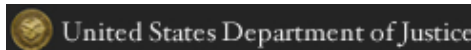
Contact:

John Marzulli

United States Attorney's Office

(718) 254-6323

Updated December 18, 2020



THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT *of* NEW YORK

[U.S. Attorneys](#) » [Eastern District of New York](#) » [News](#)

Department of Justice

U.S. Attorney's Office

Eastern District of New York

FOR IMMEDIATE RELEASE

Wednesday, December 30, 2020

Ticketmaster Pays \$10 Million Criminal Fine for Intrusions into Competitor's Computer Systems

Ticketmaster Used Passwords Unlawfully Retained by a Former Employee of a Competitor to Access Computer Systems in Scheme to "Choke Off" the Victim's Business

Earlier today in federal court in Brooklyn, Ticketmaster L.L.C. (Ticketmaster or the Company) agreed to pay a \$10 million fine to resolve charges that it repeatedly accessed without authorization the computer systems of a competitor. The fine is part of a deferred prosecution agreement that Ticketmaster has entered with the United States Attorney's Office for the Eastern District of New York to resolve a five-count criminal information filed today charging computer intrusion and fraud offenses. Previously, on October 18, 2019, Zeeshan Zaidi, the former head of Ticketmaster's Artist Services division, pled guilty in a related case to conspiring to commit computer intrusions and wire fraud based on his participation in the same scheme. Both cases are assigned to U.S. District Judge Margo K. Brodie.

Seth D. DuCharme, Acting United States Attorney for the Eastern District of New York, and William F. Sweeney, Jr., Assistant Director-in-Charge of the Federal Bureau of Investigation's New York Field Office, made the announcement.

"Ticketmaster employees repeatedly – and illegally – accessed a competitor's computers without authorization using stolen passwords to unlawfully collect business intelligence," stated Acting U.S. Attorney DuCharme. "Further, Ticketmaster's employees brazenly held a division-wide 'summit' at which the stolen passwords were used to access the victim company's computers, as if that were an appropriate business tactic. Today's resolution demonstrates that any company that obtains a competitor's confidential information for commercial advantage, without authority or permission, should expect to be held accountable in federal court."

"When employees walk out of one company and into another, it's illegal for them to take proprietary information with them. Ticketmaster used stolen information to gain an advantage over its competition, and then promoted the employees who broke the law. This investigation is a perfect example of why these laws exist - to protect consumers from being cheated in what should be a fair market place," stated FBI Assistant Director-in-Charge Sweeney.

The Scheme to "Choke Off" the Victim Company

According to Ticketmaster's admissions and publicly filed court documents, Ticketmaster, a wholly owned subsidiary of Live Nation Entertainment, Inc. (Live Nation), was primarily engaged in the business of selling and distributing tickets to events and concerts. The victim company offered artists the ability to sell presale tickets –

sold in advance of general ticket sales – on an online ticketing platform. It also offered artists an Artist Toolbox (the Toolbox), which was a password-protected app that provided real-time data about tickets sold through the victim company.

Instrumental to the criminal scheme was Coconspirator-1, a former senior employee of the victim company, who worked in the company's Brooklyn, New York offices from approximately May 2010 to July 2012. In approximately July 2012, Coconspirator-1 signed a separation agreement with the victim company, in which he agreed to maintain the confidentiality of that company's confidential information. He then joined Live Nation in approximately August 2013.

In November 2013, while employed by Live Nation, Coconspirator-1 shared with Zaidi and another Ticketmaster employee the URLs for draft ticketing web pages that the victim company had built for an artist, but had not disseminated to the public. In response to a Ticketmaster executive explaining that the goal was to “choke off [victim company]” and “steal back one of [victim company]’s signature clients,” Coconspirator-1 offered that Ticketmaster could “cut [victim company] off at the knees” if they could win back presale ticketing business for a second major artist that was a client of the victim company.

Ticketmaster's Intrusions Into the Victim Company's Password-Protected Artist Toolboxes

In January 2014, Coconspirator-1 emailed Zaidi and a second Ticketmaster executive multiple sets of usernames and passwords for Toolboxes. Coconspirator-1 encouraged the executives to “screen-grab the hell out of the system,” but also warned, “*I must stress that as this is access to a live [victim company] tool I would be careful in what you click on as it would be best not [to] giveaway that we are snooping around.*” (Emphasis in original.) The information from the Toolboxes was then used to prepare a presentation for other senior executives that was intended to “benchmark” Ticketmaster's offerings against those of the victim company.

In early May 2014, a senior executive of Live Nation (Corporate Officer-1) asked Zaidi and others how Ticketmaster's presale online offering compared with the Toolbox. Coconspirator-1 was then asked to “do a screenshare/demo” at an upcoming “Artist Services Summit.” Coconspirator-1 agreed to “pull together a list of the log-ins and URL's that I still have access to for this so I can give the team as much insight as possible.” At least 14 Live Nation and Ticketmaster employees attended the Artist Services Summit, in San Francisco. There, in front of those employees, Coconspirator-1 used a username and password he had retained from his employment at the victim company to log in to a Toolbox, and provided a demonstration. Coconspirator-1 later also provided Zaidi and other Ticketmaster executives with internal and confidential financial documents he had retained from his employment at the victim company.

In January 2015, Coconspirator-1 was transferred to the Artist Services division, promoted to Director of Client Relations, and given a raise. Following the promotion, Coconspirator-1 emailed another Artist Services employee, “Now we can really start to bring down the hammer on [Victim Company].” Ticketmaster employees continued to access password-protected victim company Toolboxes through December 2015.

Ticketmaster's Surveillance of the Victim Company's Draft Ticketing Web Pages

Between approximately July 2014 and June 2015, Coconspirator-1 and others monitored draft ticketing web pages created by the victim company. Although these pages were not password-protected, they were not indexed in search engines, and therefore could not be located without determining the exact URLs, which included a series of numbers. Until the victim company or artist publicly disseminated a URL, the victim company intended to restrict access to itself and the artist.

After joining Live Nation, Coconspirator-1 explained to Zaidi and others how the “store ID” numbers in the URLs were numbered sequentially, enabling Ticketmaster employees to monitor new pages and to learn which artists planned to use the victim company to sell tickets. Coconspirator-1 used this information to search for new victim company ticketing web pages, and sent the URLs to Ticketmaster executives. In or about January 2015, a Ticketmaster employee was assigned to learn about this system from Coconspirator-1, and maintained a spreadsheet listing every victim company ticketing web page that could be located, so that Ticketmaster could

identify the victim company's clients and attempt to dissuade them from selling tickets through the victim company. Zaidi explained that "we're not supposed to tip anyone off that we have this view into [the victim company's] activities."

The Deferred Prosecution Agreement and Criminal Information

Under the terms of the deferred prosecution agreement, Ticketmaster will pay a criminal penalty of \$10 million and will maintain a compliance and ethics program designed to prevent and detect violations of the Computer Fraud and Abuse Act and other applicable laws, and to prevent the unauthorized and unlawful acquisition of confidential information belonging to its competitors. Ticketmaster will also report to the United States Attorney's Office annually during the three-year term of the agreement regarding these compliance measures. If the Company breaches the agreement, it will be subject to prosecution for the charges in the criminal information that was filed today, charging the Company with one count of conspiracy to commit computer intrusions, one count of computer intrusion for commercial advantage, one count of computer intrusion in furtherance of fraud, one count of wire fraud conspiracy and one count of wire fraud.

The investigation is being conducted by the FBI's New York Field Office. The government's case is being handled by the Office's National Security and Cybercrime Section. Assistant United States Attorneys Allon Lifshitz, Craig R. Heeren and Ian C. Richardson are in charge of the prosecution.

The Defendants:

TICKETMASTER L.L.C.

E.D.N.Y. Docket No. 20-CR-563 (MKB)

ZEESHAN ZAIDI

Age: 46

New York, New York

E.D.N.Y. Docket No. 19-CR-450 (MKB)

Attachment(s):

[Download ticketmaster_dpa.pdf](#)

Topic(s):

Cybercrime

Component(s):

[USAO - New York, Eastern](#)

Contact:

John Marzulli

United States Attorney's Office

(718) 254-6323

Updated December 30, 2020



THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT *of* NEW YORK

U.S. Attorneys » Eastern District of New York » News

Department of Justice

U.S. Attorney's Office

Eastern District of New York

FOR IMMEDIATE RELEASE

Tuesday, January 19, 2021

Political Scientist Author Charged with Acting as an Unregistered Agent of The Iranian Government

Defendant Lobbied U.S. Officials, Published Books and Articles Advancing Iranian Viewpoints While Secretly Employed by the Iranian Mission to the United Nations

BROOKLYN, NY – A criminal complaint was unsealed today in federal court in Brooklyn charging Kaveh Lotfolah Afrasiabi, also known as “Lotfolah Kaveh Afrasiabi,” with acting and conspiring to act as an unregistered agent of the Government of the Islamic Republic of Iran, in violation of the Foreign Agents Registration Act (FARA). Afrasiabi was arrested yesterday at his home in Watertown, Massachusetts, and will make his initial appearance this morning in federal court in Boston, Massachusetts, before United States Magistrate Judge Jennifer C. Boal.

Seth D. DuCharme, Acting U.S. Attorney for the Eastern District of New York; John C. Demers, Assistant Attorney General for National Security; William F. Sweeney, Jr., Assistant Director-in-Charge, Federal Bureau of Investigation, New York Field Office (FBI); and Joseph Bonavolonta, Special Agent-in-Charge, FBI, Boston Field Office announced the arrest and charges.

“Afrasiabi allegedly sought to influence the American public and American policymakers for the benefit of his employer, the Iranian government, by disguising propaganda as objective policy analysis and expertise,” stated Acting U.S. Attorney DuCharme. “This Office is committed to the robust enforcement of the Foreign Agents Registration Act, which provides the American people the tools they need to evaluate opinions and arguments in the marketplace of ideas by requiring foreign agents to declare their paymasters. Those, like the defendant, who conceal the full extent of their work for a foreign government when the law requires disclosure will face consequences for their actions.”

“For over a decade, Kaveh Afrasiabi pitched himself to Congress, journalists, and the American public as a neutral and objective expert on Iran,” stated Assistant Attorney General Demers. “However, all the while, Afrasiabi was actually a secret employee of the Government of Iran and the Permanent Mission of the Islamic Republic of Iran to the United Nations (IMUN) who was being paid to spread their propaganda. In doing so, he intentionally avoided registering with Department of Justice as the Foreign Agents Registration Act required. He likewise evaded his obligation to disclose who was sponsoring his views. We now begin to hold him responsible for those deeds.”

“Anyone working to advance the agenda of a foreign government within the United States is required by law to register as an agent of that country,” stated FBI Assistant Director-in-Charge Sweeney. “Mr. Afrasiabi never disclosed to a Congressman, journalists or others who hold roles of influence in our country that he was being paid by the Iranian government to paint an untruthfully positive picture of the nation. Our laws are designed to create

transparency in foreign relations, and they are not arbitrary or malleable. As today's action demonstrates, we will fully enforce them to protect our national security."

"Our arrest of Kaveh Afrasiabi makes it clear that the United States is not going to allow undeclared agents of Iran to operate in our country unchecked. For more than a decade, Mr. Afrasiabi was allegedly paid, directed, and controlled by the Government of Iran to lobby U.S. government officials, including a Congressman; and to create and disseminate information favorable to the Iranian government," stated FBI Special Agent-in-Charge Bonavolonta. "The FBI will continue to do everything it can to uncover these hidden efforts and hold accountable those who work for our adversaries to the detriment of our national security."

According to the complaint, Afrasiabi is a citizen of the Islamic Republic of Iran and a lawful permanent resident of the United States. Afrasiabi holds a PhD, and frequently publishes books and articles, and appears on English-language television programs discussing foreign relations matters, particularly Iran's relations with the United States. Afrasiabi has identified or portrayed himself as a political scientist, a former political science professor or as an expert on foreign affairs.

Since at least 2007 to the present, Afrasiabi has also been secretly employed by the Iranian government and paid by Iranian diplomats assigned to the Permanent Mission of the Islamic Republic of Iran to the United Nations in New York City (IMUN). Afrasiabi has been paid approximately \$265,000 in checks drawn on the IMUN's official bank accounts since 2007 and has received health insurance through the IMUN's employee health benefit plans since at least 2011.

In the course of his employment by the Iranian government, Afrasiabi has lobbied a U.S. Congressman and the U.S. Department of State to advocate for policies favorable to Iran, counseled Iranian diplomats concerning U.S. foreign policy, made television appearances to advocate for the Iranian government's views on world events, and authored articles and opinion pieces espousing the Iranian government's position on various matters of foreign policy. Afrasiabi has long known that FARA requires agents of foreign principals to register with the U.S. Department of Justice and has discussed information obtained from FARA disclosures with others. Nevertheless, Afrasiabi did not register as an agent of the Government of Iran.

For example, in January 2020, Afrasiabi emailed Iran's Foreign Minister and Permanent Representative to the United Nations with advice for "retaliation" for the U.S. military airstrike that killed Major General Qasem Soleimani, the head of the Quds Force, the external operations arm of the Iranian government's Islamic Revolutionary Guard Corps, proposing that the Iranian government "end all inspections and end all information on Iran's nuclear activities pending a [United Nations Security Council] condemnation of [the United States'] illegal crime." Afrasiabi claimed that such a move would, among other things, "strike fear in the heart of [the] enemy."

Afrasiabi has admitted in his own communications that his extensive body of published works and television appearances, in which he has consistently advocated perspectives and policy positions favored by the Iranian government, has been attributable to the funding he receives from the Iranian government. For example, in a July 28, 2020 email to Iran's Foreign Minister, Afrasiabi included "links for many of [his] works, including books, hundreds of articles in international newspapers and academic journals," telling Iran's Foreign Minister "Without support none of this would have been possible! This has been a very productive relationship spanning decades that ought not to be interrupted."

The charges in the complaint are allegations, and the defendant is presumed innocent unless and until proven guilty. If convicted of both charged offenses, Afrasiabi faces a maximum sentence of 10 years in prison.

The government's case is being handled by the Office's National Security and Cybercrime Section. Assistant United States Attorneys Ian C. Richardson and Michael T. Keilty are in charge of the prosecution, with assistance from Trial Attorney David C. Recker of the National Security Division's Counterintelligence and Export Control Section.

The Defendant:

KAVEH LOTFOLAH AFRASIABI (also known as "Lotfolah Kaveh Afrasiabi")

Age: 63

Watertown, Massachusetts

E.D.N.Y. Docket No. 21-MJ-50

Attachment(s):

[Download Kaveh Afrasiabi Complaint](#)

Topic(s):

National Security

Component(s):

[USAO - New York, Eastern](#)

Contact:

John Marzulli

United States Attorney's Office

(718) 254-6323

Updated January 19, 2021



THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT *of* NEW YORK

[U.S. Attorneys](#) » [Eastern District of New York](#) » [News](#)

Department of Justice

U.S. Attorney's Office

Eastern District of New York

FOR IMMEDIATE RELEASE

Monday, November 22, 2021

Queens Man Sentenced to 19 Months in Prison for Threatening to Murder Members of Congress

Brendan Hunt Threatened to “Slaughter” Senators and Representatives Two Days After the January 6, 2021 Storming of the U.S. Capitol

Earlier today, at the federal courthouse in Brooklyn, Brendan Hunt was sentenced by United States District Judge Pamela K. Chen to 19 months' imprisonment for threatening to assault and murder members of the United States Congress to impede, interfere with and intimidate those members and to retaliate against them on account of their performance of their official duties. Hunt was convicted of that charge after a jury trial in April 2021, which was the first trial to address the consequences of the January 6, 2021 assault on the Capitol.

Breon Peace, United States Attorney for the Eastern District of New York, and Michael J. Driscoll, Assistant Director-in-Charge, Federal Bureau of Investigation, New York Field Office (FBI), announced the sentence.

“We will not tolerate threats to members of the United States Congress or calls to overthrow our democratically elected government,” stated United States Attorney Peace. “Not only will we investigate and vigorously prosecute these crimes, but today's sentence sends a clear message that those who seek to harm our representatives and bring chaos to our democracy will be punished.”

On January 8, 2021, two days after the violent attack on the U.S. Capitol in Washington, D.C., Hunt posted a video titled “KILL YOUR SENATORS” that included the summary “Slaughter them all,” to BitChute, an Internet-based video sharing site. In the video, Hunt made dangerous additional threats, exhorting his viewers to violence and telling them that “[w]e need to go back to the U.S. Capitol when all of the Senators and a lot of the Representatives are back there, and this time we have to show up with our guns. And we need to slaughter these m-----f-----s.” Hunt also advocated for the violent overthrow of the federal government, claiming that “our government at this point is basically a handful of traitors . . . so what you need to do is take up arms, get to D.C., probably the inauguration . . . so called inauguration of this m-----f-----g communist Joe Biden . . . [T]hat's probably the best time to do this, get your guns, show up to D.C., and literally just spray these m-----f-----s . . . put some bullets in their f-----g heads.” Hunt stated, “If anybody has a gun, give me it, I'll go there myself and shoot them and kill them . . . [W]e have to take out these Senators and then replace them with actual patriots. This is a [Zionist Occupied Government].”

On January 9, 2021, the defendant posted another video in which he stated “[t]hose 100 Senators should really be afraid about going into public now” and that “We have the first amendment, that's still around, remember? And we have the second as well. There are really only a hundred of these weakling Senators. They are mass murdering

psychopaths who are intent on our destruction, and they form an illegitimate government. Every single one of them just needs to go.”

The government's case is being handled by the Office's National Security and Cybercrime Section. Assistant United States Attorneys David K. Kessler, Ian C. Richardson and Francisco J. Navarro are in charge of the prosecution.

The Defendant:

BRENDAN HUNT

Age: 37

Ridgewood, Queens

E.D.N.Y. Docket No. 21-CR-086 (PKC)

Topic(s):

National Security

Violent Crime

Component(s):

USAO - New York, Eastern

Contact:


John Marzulli

United States Attorney's Office

(718) 254-6323

Updated November 22, 2021

EXHIBIT G

 An official website of the United States government
[Here's how you know](#)



Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, April 17, 2019

Former Manager for International Airline Pleads Guilty to Acting as an Agent of the Chinese Government

Defendant Placed Packages on Flights from JFK Airport to Beijing at the Direction of Military Officers Assigned to the Chinese Mission to the United Nations

Earlier today, in federal court in Brooklyn, New York, Ying Lin pleaded guilty to acting as an agent of the People's Republic of China (PRC), without notification to the Attorney General, by working at the direction and control of military officers assigned to the Permanent Mission of the People's Republic of China to the United Nations. Lin, a former manager with an international air carrier headquartered in the PRC (the Air Carrier), abused her privileges to transport packages from John F. Kennedy International Airport (JFK Airport) to the PRC aboard Air Carrier flights at the behest of the PRC military officers and in violation of Transportation Security Administration (TSA) regulations. The proceeding was held before United States District Judge Ann M. Donnelly.

Assistant Attorney General for National Security John C. Demers, U.S. Attorney Richard P. Donoghue for the Eastern District of New York, Assistant Director in Charge William F. Sweeney, Jr of the FBI's New York Field Office, and Special Agent in Charge Angel M. Melendez, Department of Homeland Security, Homeland Security Investigations (HSI) announced the guilty plea.

"This case is a stark example of the Chinese government using the employees of Chinese companies doing business here to engage in illegal activity," said Assistant Attorney General Demers. "Covertly doing the Chinese military's bidding on U.S. soil is a crime, and Lin and the Chinese military took advantage of a commercial enterprise to evade legitimate U.S. government oversight."

"The defendant's actions as an agent of the Chinese government helped Chinese military officers to evade U.S. law enforcement scrutiny of packages that they sent from New York to Beijing," stated United States Attorney Donoghue. "This case demonstrates how seriously we address counterintelligence threats posed by individuals in the United States who work for foreign governments, such as China."

"The FBI and our law enforcement partners do all we can every day to protect this country from the threats we can see, and we work even harder to find the threats we can't see," said FBI Assistant Director-in-Charge Sweeney. "Ms. Lin was secreting packages through some of the country's busiest airports, using her work with the Chinese government to thwart our security measures. We believe this case isn't unique and hope it serves as an example that the Chinese and other foreign governments can't break our laws with impunity."

"Lin's criminal actions exploited the international boundary of the United States as she used her position to smuggle packages onto planes headed to China," said HSI Special Agent-in-Charge Melendez. "We are committed to ensuring the integrity of our international airports so they are not used as a front for illicit activities."

Lin worked for the Air Carrier from 2002 through the fall of 2015 as a counter agent at JFK Airport and from the fall of 2015 through April 2016 as the station manager at Newark Liberty International Airport. During her employment with the Air Carrier, Lin accepted packages from the PRC military officers, and placed those packages aboard Air Carrier flights to the PRC as unaccompanied luggage or checked in the packages under the names of other passengers flying on those flights. As the

PRC military officers did not travel on those flights, Lin's actions were contrary to a security program that required that checked baggage be accepted only from ticketed passengers, thereby violating TSA regulations. In addition, Lin encouraged other Air Carrier employees to assist the PRC military officers, instructing those employees that because the Air Carrier was a PRC company, their primary loyalty should be to the PRC.

In exchange for her work at the direction and under the control of PRC military officers and other PRC government officials, Lin received benefits from the PRC Mission and PRC Consulate in New York. These benefits included tax-exempt purchases of liquor, cigarettes and electronic devices worth tens of thousands of dollars. These benefits also included free contracting work at the defendant's two residences in Queens, New York, by PRC construction workers who were permitted under the terms of their visas to work only on PRC government facilities.

When sentenced, Lin faces up to 10 years' imprisonment. As part of the guilty plea, Lin agreed to forfeit approximately \$25,000 as well as an additional \$145,000 in connection with her resolution of the government's forfeiture verdict in United States v. Zhong, No. 16-CR-614 (AMD).

Mr. Demers and Mr. Donoghue expressed their appreciation to the Transportation Security Administration for their assistance on the case. The government's case is being handled by the National Security and Cybercrime Section. Assistant United States Attorneys Douglas M. Pravda, Alexander A. Solomon, Ian C. Richardson and Sarah M. Evans are in charge of the prosecution, with assistance from Trial Attorney Matthew R. Walczewski of the Department of Justice's Counterintelligence and Export Control Section. The forfeiture aspect of the case is being handled by EDNY Assistant United States Attorney Brian Morris of the Office's Civil Division.

Topic(s):

Counterintelligence and Export Control

Component(s):

Federal Bureau of Investigation (FBI).


National Security Division (NSD).

USAO - New York, Eastern

Press Release Number:

19-393

Updated April 17, 2019

 An official website of the United States government
[Here's how you know](#)



Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Friday, October 18, 2019

Chinese National Sentenced to 40 Months in Prison for Conspiring to Illegally Export Military- and Space-Grade Technology from the United States to China

On October 16, 2019, United States District Judge Diane J. Humetewa sentenced Tao Li, a 39-year-old Chinese national, to 40 months in prison, followed by three years of supervised release. Li had previously pleaded guilty to conspiring to export military- and space-grade technology to the People's Republic of China without a license in violation of the International Emergency Economic Powers Act.

"This case is one of many involving illegal attempts to take U.S. technology to China. Li attempted to procure highly sensitive U.S. military technology in violation of our export control laws. Such laws are in place to protect our national security, and the Department of Justice will continue to vigorously enforce them," said Assistant Attorney General John C. Demers. "We don't take these crimes lightly and we will continue to pursue them."

"If you steal our military and space technology, you should expect to go to prison," said Michael Bailey, United States Attorney for the District of Arizona. "But for the diligent work of HSI and the Defense Criminal Investigative Service, our nation's security would've been damaged by Mr. Li."

"Li's sentencing was the result of a highly successful joint investigative effort with our law enforcement partners and the U.S. Attorney's Office that prevented U.S. military technology from falling into the wrong hands," said Bryan D. Denny, Special Agent in Charge of the Defense Criminal Investigative Service, Western Field Office. "It also reaffirms our commitment to protecting America from this type of activity and, equally so, serves as a warning to those intent on illegally exporting our technologies that the Defense Criminal Investigative Service and its partners will pursue these crimes relentlessly."

"This sentence is well deserved and further demonstrates the lengths of criminal activity by those who seek to engage in illegally obtaining sophisticated materials," said Scott Brown, Special Agent in Charge for Homeland Security Investigations (HSI) Phoenix. "One of HSI's top priorities is preventing U.S. military products and sensitive technology from falling into the hands of those who might seek to harm America or its interests. We will continue to aggressively pursue violators wherever they may be."

Between December 2016 and January 2018, Li worked with other individuals in China to purchase radiation-hardened power amplifiers and supervisory circuits and illegally export them from the United States to China. The electronic components sought by Li are capable of withstanding significant levels of radiation and extreme heat, and as a result, are primarily used for military and space applications. Due to the technological capabilities of the electronic components sought by Li and the significant contribution that the components could make to a foreign country's military and space programs, both parts required an export license from the U.S. Department of Commerce, Bureau of Industry and Security, prior to being sent out of the United States. Notwithstanding the licensing requirement, the Department of Commerce has a policy of denial to export these types of electronic components to the People's Republic of China.

Between December 2016 and January 2018, Li, who resided in China, used multiple aliases to contact individuals in the United States, including representatives of United States-based private companies, to try to obtain the electronic components. Additionally, Li and his coconspirators agreed to pay a "risk fee" to illegally export the electronic components to China. In furtherance of his request, Li wired money from a bank account in China to a bank account in Arizona. Li was arrested in September 2018 at Los Angeles International Airport, as Li attempted to travel from China to Arizona to meet with one of the undercover agents.

The investigation in this case was conducted by HSI and DCIS. The prosecution was handled by Todd M. Allison and David Pimsner, Assistant United States Attorneys, District of Arizona, Phoenix, with assistance from Scott Claffee, Trial Attorney, Department of Justice National Security Division.

Topic(s):

Counterintelligence and Export Control
National Security


Component(s):

National Security Division (NSD)
USAO - Arizona

Press Release Number:

19-1118

Updated October 18, 2019

 An official website of the United States government
[Here's how you know](#)



Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Monday, August 17, 2020

Former CIA Officer Arrested and Charged with Espionage

Alexander Yuk Ching Ma, 67, a former Central Intelligence Agency (CIA) officer, was arrested on Aug. 14, 2020, on a charge that he conspired with a relative of his who also was a former CIA officer to communicate classified information up to the Top Secret level to intelligence officials of the People's Republic of China (PRC). The Criminal Complaint containing the charge was unsealed this morning.

Assistant Attorney General for National Security John C. Demers, U.S. Attorney for the District of Hawaii Kenji M. Price, Assistant Director of the FBI's Counterintelligence Division Alan E. Kohler Jr., and Special Agent in Charge of the FBI's Honolulu Field Office Eli S. Miranda made the announcement.

"The trail of Chinese espionage is long and, sadly, strewn with former American intelligence officers who betrayed their colleagues, their country and its liberal democratic values to support an authoritarian communist regime," said Assistant Attorney General for National Security John C. Demers. "This betrayal is never worth it. Whether immediately, or many years after they thought they got away with it, we will find these traitors and we will bring them to justice. To the Chinese intelligence services, these individuals are expendable. To us, they are sad but urgent reminders of the need to stay vigilant."

"The charges announced today are a sobering reminder to our communities in Hawaii of the constant threat posed by those who seek to jeopardize our nation's security through acts of espionage," said U.S. Attorney Price. "Of particular concern are the criminal acts of those who served in our nation's intelligence community, but then choose to betray their former colleagues and the nation-at large by divulging classified national defense information to China. My office will continue to tenaciously pursue espionage cases."

"This serious act of espionage is another example in a long string of illicit activities that the People's Republic of China is conducting within and against the United States," said Alan E. Kohler Jr., Assistant Director of the FBI's Counterintelligence Division. "This case demonstrates that no matter the length or difficulty of the investigation, the men and women of the FBI will work tirelessly to protect our national security from the threat posed by Chinese intelligence services. Let it be known that anyone who violates a position of trust to betray the United States will face justice, no matter how many years it takes to bring their crimes to light."

"These cases are very complicated and take years if not decades to bring to a conclusion," said Eli Miranda, Special Agent in Charge of the FBI's Honolulu Division. "I could not be more proud of the work done by the men and women of the FBI's Honolulu Division in pursuing this case. Their dedication is a reminder that the FBI will never waiver when it comes to ensuring the safety and security of our nation."

Ma is a naturalized U.S. citizen born in Hong Kong. According to court documents, Ma began working for the CIA in 1982, maintained a Top Secret clearance, and signed numerous non-disclosure agreements in which he acknowledged his responsibility and ongoing duty to protect U.S. government secrets during his tenure at CIA. Ma left the CIA in 1989 and lived and worked in Shanghai, China before arriving in Hawaii in 2001.

According to court documents, Ma and his relative (identified as co-conspirator #1) conspired with each other and multiple PRC intelligence officials to communicate classified national defense information over the course of a decade. The scheme began with three days of meetings in Hong Kong in March 2001 during which the two former CIA officers provided information to the foreign intelligence service about the CIA's personnel, operations, and methods of concealing communications. Part of

the meeting was captured on videotape, including a portion where Ma can be seen receiving and counting \$50,000 in cash for the secrets they provided.

The court documents further allege that after Ma moved to Hawaii, he sought employment with the FBI in order to once again gain access to classified U.S. government information which he could in turn provide to his PRC handlers. In 2004, the FBI's Honolulu Field Office hired Ma as a contract linguist tasked with reviewing and translating Chinese language documents. Over the following six years, Ma regularly copied, photographed and stole documents that displayed U.S. classification markings such as "SECRET." Ma took some of the stolen documents and images with him on his frequent trips to China with the intent to provide them to his handlers. Ma often returned from China with thousands of dollars in cash and expensive gifts, such as a new set of golf clubs.

According to court documents, in spring 2019, over the course of two in-person meetings, Ma confirmed his espionage activities to an FBI undercover employee Ma believed was a representative of the PRC intelligence service, and accepted \$2,000 in cash from the FBI undercover as "small token" of appreciation for Ma's assistance to China. Ma also offered to once again work for the PRC intelligence service. On August 12, 2020, during a meeting with an FBI undercover employee before arrest, Ma again accepted money for his past espionage activities, expressed his willingness to continue to help the Chinese government, and stated that he wanted "the motherland" to succeed.

Ma will make his initial appearance before a federal judge tomorrow in the U.S. District Court for the District of Hawaii. He is charged with conspiracy to communicate national defense information to aid a foreign government and faces a maximum penalty of life imprisonment if convicted. The maximum sentence is prescribed by Congress and is provided here for informational purposes. In the event Ma is convicted, a federal district court judge will determine any sentence after taking into account the advisory Sentencing Guidelines and other statutory factors.

The investigation was conducted by the FBI's Honolulu and Los Angeles Field Offices. Assistant U.S. Attorney Ken Sorenson and Trial Attorneys Scott Claffee and Steve Marzen of the National Security Division's Counterintelligence and Export Control Section are prosecuting the case.

Attachment(s):

[Download ma_complaint_.pdf](#)

Topic(s):

Counterintelligence and Export Control
National Security

Component(s):

[National Security Division \(NSD\)](#)
[USAO - Hawaii](#)

Press Release Number:

20-789

Updated December 7, 2020



THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT *of* NEW YORK

U.S. Attorneys » Eastern District of New York » News

Department of Justice

U.S. Attorney's Office

Eastern District of New York

FOR IMMEDIATE RELEASE

Monday, September 21, 2020

**New York City Police Department Officer Charged with Acting as an
Illegal Agent of the People's Republic of China**

**The Defendant Reported to Officials with the PRC Consulate About the Activities of Chinese
Citizens in the New York Area and Assessed Potential Intelligence Sources for the PRC
Within the Tibetan Community in New York and Elsewhere**

BROOKLYN, NY – A criminal complaint was unsealed today in federal court in Brooklyn charging Baimadajie Angwang, a New York City Police Department officer and United States Army reservist, with acting as an illegal agent of the People's Republic of China (PRC) as well as committing wire fraud, making false statements and obstructing an official proceeding. Angwang was arrested today and will make his initial appearance this afternoon before United States Magistrate Judge Roanne L. Mann.

Seth D. DuCharme, Acting United States Attorney for the Eastern District of New York; John C. Demers, Assistant Attorney General for National Security; Alan E. Kohler, Jr., Assistant Director of the Federal Bureau of Investigation (FBI) Counterintelligence Division; William F. Sweeney, Jr., Assistant Director-in-Charge, Federal Bureau of Investigation, New York Field Office (FBI); and Dermot F. Shea, Commissioner, New York City Police Department (NYPD), announced the arrest and charges.

"The defendant allegedly violated his sworn oath to serve the New York City community and defend the Constitution against all enemies by reporting to PRC government officials about the activities of Chinese citizens in the New York area and developing intelligence sources within the Tibetan community in the United States," stated Acting United States Attorney DuCharme. "This Office, together with our law enforcement partners, remains vigilant in rooting out any attempts at foreign influence through criminal activity taken on behalf of a foreign power in whatever form they may take."

"State and local officials should be aware that they are not immune to the threat of Chinese espionage," said Assistant Attorney General for National Security John C. Demers. "According to the allegations, the Chinese government recruited and directed a U.S. citizen and member of our nation's largest law enforcement department to further its intelligence gathering and repression of Chinese abroad. Our police departments provide for our public safety and are often the first line of defense against the national security threats our country faces. We will continue to work with our state and local partners to protect our nation's great police departments."

"The defendant allegedly violated the trust of his community and the New York City Police Department on behalf of a foreign power, the People's Republic of China. This type of conduct simply cannot be tolerated," stated FBI Assistant Director Kohler. "This case serves as yet another reminder that China represents the biggest

counterintelligence threat to the United States and that the FBI and our partners will be aggressive in investigating and stopping such activities within our nation.”

“This is the definition of an insider threat - as alleged, Mr. Angwang operated on behalf of a foreign government; lied to gain his clearance, and used his position as an NYPD police officer to aid the Chinese government's subversive and illegal attempts to recruit intelligence sources,” stated FBI Assistant Director-in-Charge Sweeney. “The FBI is committed to stopping hostile foreign governments from infiltrating our institutions, and we will not tolerate the behavior of those who willingly violate their oath to the United States, and covertly work against their fellow citizens. We want to thank the NYPD for its extraordinary partnership on this investigation.”

“As alleged in this federal complaint, Baimadajie Angwang violated every oath he took in this country. One to the United States, another to the U.S. Army, and a third to this Police Department,” stated NYPD Commissioner Shea. “From the earliest stages of this investigation, the NYPD’s Intelligence and Internal Affairs bureaus worked closely with the FBI’s Counterintelligence Division to make sure this individual would be brought to justice.”

According to the publicly filed complaint and the government’s detention memorandum, Angwang, an ethnic Tibetan native of the PRC and naturalized U.S. citizen, is assigned to the NYPD’s community affairs unit where he serves as a liaison to the community served by the 111th Precinct.

Since at least 2014, Angwang allegedly acted at the direction and control of officials at the PRC Consulate in New York City. Specifically, Angwang reported on the activities of Chinese citizens in the New York area, spotted and assessed potential intelligence sources within the Tibetan community in New York and elsewhere, and provided PRC officials with access to senior NYPD officials through invitations to official events. One of the PRC Consular officials at whose direction Angwang acted worked for the China Association for Preservation and Development of Tibetan Culture, a division of the PRC’s United Front Work Department. This Department is responsible for, among other things, neutralizing potential opponents of the PRC and co-opting ethnic Chinese individuals living outside the PRC.

Angwang is also charged with committing wire fraud, making material false statements and obstructing an official proceeding. As part of his employment with the U.S. Army Reserve, Angwang maintained a “SECRET”-level security clearance. According to court documents, in 2019, Angwang completed and electronically submitted an SF-86C form for a background investigation. On the form, Angwang lied by denying that he had contacts with a foreign government or its consulate and by denying that he had close and continuing contacts with foreign nationals, including his family members who live in the PRC, some of whom are affiliated with the People’s Liberation Army.

The charges in the complaint are allegations, and the defendant is presumed innocent unless and until proven guilty. If convicted, Angwang faces a maximum sentence of 55 years’ imprisonment.

The government’s case is being handled by the Office’s National Security and Cybercrime Section. Assistant United States Attorney Michael T. Keilty is in charge of the prosecution, with assistance from Trial Attorney Scott A. Claffee of the National Security Division’s Counterintelligence and Export Control Section.

The Defendant:

BAIMADAJIE ANGWANG

Age: 33

Williston Park, New York

E.D.N.Y. Docket No. 20-MJ-837

Attachment(s):

[Download Angwang Complaint](#)

Topic(s):

Component(s):

USAO - New York, Eastern


Contact:

John Marzulli

United States Attorney's Office

(718) 254-6323

Updated September 21, 2020

 An official website of the United States government
[Here's how you know](#)



Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, October 28, 2020

Eight Individuals Charged With Conspiring to Act as Illegal Agents of the People's Republic of China

PRC Officials Directed Multi-Year Campaign of Harassment and Stalking; Directed at U.S. Residents to Force Their Return to PRC

A complaint and arrest warrants were unsealed today in federal court in Brooklyn charging eight defendants with conspiring to act in the United States as illegal agents of the People's Republic of China (PRC). Six defendants also face related charges of conspiring to commit interstate and international stalking. The defendants, allegedly acting at the direction and under the control of PRC government officials, conducted surveillance of and engaged in a campaign to harass, stalk, and coerce certain residents of the United States to return to the PRC as part of a global, concerted, and extralegal repatriation effort known as "Operation Fox Hunt."

Zhu Yong, Hongru Jin, and Michael McMahon were arrested today and will be arraigned this afternoon via teleconference before U.S. Magistrate Judge Peggy Kuo. Rong Jing and Zheng Congying were arrested in the Central District of California, and their initial appearances will take place in that district later today. Zhu Feng, Hu Ji, and Li Minjun remain at large.

"With today's charges, we have turned the PRC's Operation Fox Hunt on its head — the hunters became the hunted, the pursuers the pursued," said Assistant Attorney General for National Security John C. Demers. "The five defendants the FBI arrested this morning on these charges of illegally doing the bidding of the Chinese government here in the United States now face the prospect of prison. For those charged in China and others engaged in this type of conduct, our message is clear: stay out. This behavior is not welcome here."

"The Chinese government's brazen attempts to surveil, threaten, and harass our own citizens and lawful permanent residents, while on American soil, are part of China's diverse campaign of theft and malign influence in our country and around the world," said FBI Director Christopher Wray. "The FBI will use all of its tools to investigate and defeat these outrageous actions by the Chinese government, which are an affront to America's ideals of freedom, human rights, and the rule of law."

"As alleged, the defendants assisted PRC officials in a scheme to coerce targeted individuals to return to the PRC against their will," said Acting U.S. Attorney Seth D. DuCharme. "The United States will not tolerate the conduct of PRC carrying out state-authorized actions on U.S. soil without notice to, and coordination with, the appropriate U.S. authorities. Nor will we tolerate the unlawful harassment and stalking of U.S. residents to further PRC objectives." Acting U.S. Attorney DuCharme also extended his thanks and appreciation to the FBI's Los Angeles Field Office for their work on the case.

"Today's announcement of these charges further highlights the FBI's ongoing and aggressive commitment to investigate China's efforts to illegally impose its will in the United States", said Special Agent in Charge George M. Crouch Jr. of the FBI Newark Field Office. "This case should serve as a reminder to the People's Republic of China that when it directs criminal activity within our borders, the FBI and its law enforcement partners will make sure the perpetrators are held accountable."

"The worldwide presence and investigative capabilities of the Diplomatic Security Service enables us to work with our law enforcement partners domestically and around the world to bring criminals to justice," said Keith Byrne, Special Agent in Charge of the New York Field Office of the Diplomatic Security Service.

According to the complaint, the defendants participated in an international campaign to threaten, harass, surveil and intimidate John Doe-1, a resident of New Jersey, and his family in order to force them to return to the PRC as part of an international effort by the PRC government known within the PRC as “Operation Fox Hunt” and “Operation Skynet.” In furtherance of the operation, the PRC government targets Chinese individuals living in foreign countries that the PRC government alleges have committed crimes under PRC law and seeks to repatriate them to the PRC to face charges. Rather than rely upon proper forms of international law enforcement cooperation, such as Interpol “red notices” and requests for information through appropriate governmental channels, the defendants allegedly engaged in clandestine, unsanctioned, and illegal conduct within the United States and facilitated the travel of PRC government officials (PRC Officials) to U.S. soil in order to further carry out these illegal acts. Between 2016 and 2019, multiple PRC Officials directed the defendants, and several others, to engage in efforts to coerce the victims to return to the PRC, which included the following:

Surveillance and Coercion

In April 2017, defendants Zhu Feng, Hu Ji, Li Minjun, Hongru Jin, Zhu Yong, and Michael McMahon, together with others, including the PRC Officials, allegedly participated in a scheme to bring John Doe-1’s elderly father from the PRC to the United States against the father’s will and to use the surprise arrival of his elderly father to threaten and attempt to coerce John Doe-1’s return to the PRC. Zhu Feng, Hu Ji, and Zhu Yong worked with Michael McMahon, a private investigator, to gather intelligence about and locate John Doe-1 and his wife in the United States. PRC Officials coerced the father of John Doe-1 to travel from the PRC to the New York area in the company of Li Minjun, a doctor, who traveled with the elderly father from the PRC to the New York area. Hongru Jin assisted with logistics of the operation when Zhu Feng, Li Minjun, John Doe-1’s elderly father, and other PRC officials arrived in the U.S.

As charged in the complaint, during this phase of the scheme, McMahon, whose task was to surveil John Doe-1’s father in order to locate John Doe-1 and his wife, suggested to Zhu Feng that they could “harass [John Doe-1]. Park outside his home and let him know we are there.” Later, Zhu Feng told McMahon, “[t]hey definitely grant u a nice trip if they can get [John Doe-1] back to China haha.”

The conspirators also discussed the false statements John Doe-1’s father should make to U.S. immigration authorities about the purpose of his travel to the United States. The conspirators also made efforts to destroy evidence and delete their electronic communications to avoid detection by U.S. law enforcement.

Targeting and Harassment of Victims’ Daughter

Between May 2017 and July 2018, Rong Jing and several co-conspirators allegedly targeted John Doe-1’s adult daughter for surveillance and online harassment. Specifically, Rong Jing attempted to hire a private investigator to locate John Doe-1’s adult daughter in order to photograph and video record the daughter as part of a campaign to exert pressure on John Doe-1. Around the same time, an unidentified co-conspirator sent harassing messages over social media to John Doe-1’s daughter and her friends related to the PRC’s interest in repatriating John Doe-1.

Continued Harassment of Victims

In September 2018, Zheng Congying and another unidentified co-conspirator allegedly affixed a threatening note to the door of the John Doe-1’s residence stating, “If you are willing to go back to mainland and spend 10 years in prison, your wife and children will be all right. That’s the end of this matter!” Between February 2019 and April 2019, other co-conspirators caused unsolicited packages to be sent to John Doe-1’s residence. These packages contained letters and a video with messages intended to coerce John Doe-1’s return to the PRC by threatening harm to family members still residing in the PRC.

The charges in the complaint are allegations, and the defendants are presumed innocent unless and until proven guilty. If convicted of the charged conspiracy to act as an agent of the PRC, each of the eight defendants charged today faces a maximum sentence of five years in prison. Defendants Zhu Feng, Hu Ji, Li Minjun, Michael McMahon, Rong Jing, and Zheng Congying also face an additional charge of conspiracy to commit interstate and international stalking, which carries a maximum sentence of five years in prison.

The government’s case is being handled by the Office’s National Security and Cybercrime Section. Assistant U.S. Attorneys Craig R. Heeren and J. Matthew Haggans are in charge of the prosecution, with assistance from Trial Attorney Scott A. Claffee of the National Security Division’s Counterintelligence and Export Control Section.

Attachment(s):

[Download 2020_10_28_fox_hunt_complaint.pdf](#)

[Download china_arrest_graphic_1.jpg](#)

[Download china_arrest_graphic_2.jpg](#)

[Download china_arrest_graphic_3.jpg](#)

[Download china_arrest_graphic_4.jpg](#)

Topic(s):

National Security

Component(s):

[National Security Division \(NSD\)](#)

Press Release Number:

20-1170

Updated October 29, 2020



THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT *of* NEW YORK

[U.S. Attorneys](#) » [Eastern District of New York](#) » [News](#)

Department of Justice

U.S. Attorney's Office

Eastern District of New York

FOR IMMEDIATE RELEASE

Friday, December 18, 2020

China-Based Executive at U.S. Telecommunications Company Charged with Disrupting Video Meetings Commemorating Tiananmen Square Massacre

Defendant Coordinated with the PRC Government to Target Dissidents and Disrupt Meetings

A complaint and arrest warrant were unsealed today in federal court in Brooklyn charging Xinjiang Jin, also known as "Julien Jin," with conspiracy to commit interstate harassment and unlawful conspiracy to transfer a means of identification. Jin, an employee of a U.S.-based telecommunications company (Company-1) who was based in the People's Republic of China (PRC), allegedly participated in a scheme to disrupt a series of meetings in May and June 2020 held to commemorate the June 4, 1989 Tiananmen Square massacre in the PRC. The meetings were conducted using a videoconferencing program provided by Company-1, and were organized and hosted by U.S.-based individuals, including individuals residing in the Eastern District of New York. Jin is not in U.S. custody.

Seth D. DuCharme, Acting United States Attorney for the Eastern District of New York; John C. Demers, Assistant Attorney General for National Security; and Christopher Wray, Director, Federal Bureau of Investigation (FBI), announced the charges.

"The allegations in the complaint lay bare the Faustian bargain that the PRC government demands of U.S. technology companies doing business within the PRC's borders, and the insider threat that those companies face from their own employees in the PRC," stated Acting United States Attorney DuCharme. "As alleged, Jin worked closely with the PRC government and members of PRC intelligence services to help the PRC government silence the political and religious speech of users of the platform of a U.S. technology company. Jin willingly committed crimes, and sought to mislead others at the company, to help PRC authorities censor and punish U.S. users' core political speech merely for exercising their rights to free expression. The charges announced today make clear that employees working in the PRC for U.S. technology companies make those companies—and their users—vulnerable to the malign influence of the PRC government. This Office will continue working tirelessly to protect against threats to the free expression of political views and religious beliefs, regardless whether those threats come from inside or outside the United States." Mr. DuCharme and Mr. Demers also extended their thanks and appreciation to Company-1 for its cooperation in the government's ongoing investigation.

"No company with significant business interests in China is immune from the coercive power of the Chinese Communist Party," stated Assistant Attorney General Demers. "The Chinese Communist Party will use those within its reach to sap the tree of liberty, stifling free speech in China, the United States and elsewhere about the Party's repression of the Chinese people. For companies with operations in China, like that here, this reality may

mean executives being coopted to further repressive activity at odds with the values that have allowed that company to flourish here.”

“The FBI remains committed to protecting the exercise of free speech for all Americans. As this complaint alleges, that freedom was directly infringed upon by the pernicious activities of Communist China’s Intelligence Services, in support of a regime that neither reflects nor upholds our democratic values,” stated FBI Director Wray. “Americans should understand that the Chinese Government will not hesitate to exploit companies operating in China to further their international agenda, including repression of free speech.”

According to the complaint, Jin served as Company-1’s primary liaison with PRC law enforcement and intelligence services. In that capacity, he regularly responded to requests from the PRC government for information and to terminate video meetings hosted on Company-1’s video communications platform. Part of Jin’s duties included providing information to the PRC government about Company-1’s users and meetings, and in some cases he provided information – such as Internet Protocol addresses, names and email addresses – of users located outside of the PRC. Jin was also responsible for proactively monitoring Company-1’s video communications platform for what the PRC government considers to be “illegal” meetings to discuss political and religious subjects unacceptable to the Chinese Communist Party (CCP) and the PRC government.

As alleged in the complaint, between January 2019 to the present, Jin and others conspired to use Company-1’s systems in the United States to censor the political and religious speech of individuals located in the United States and around the world at the direction and under the control of officials of the PRC government. Among other actions taken at the direction of the PRC government, Jin and others terminated at least four video meetings hosted on Company-1’s networks commemorating the thirty-first anniversary of the Tiananmen Square massacre, most of which were organized and attended by U.S.-based participants, such as dissidents who had participated in and survived the 1989 protests. Some of the participants who were unable to attend these meetings were Company-1 customers in Queens and Long Island, New York who had purchased subscriptions to Company-1’s services, and therefore entered into service agreements with Company-1 governed by its Terms of Service (TOS).

Jin, officials from the PRC government and others allegedly collaborated to identify meeting participants and to disrupt meetings hosted on Company-1’s U.S. servers, at times creating pretextual reasons to justify their actions to other employees and executives of Company-1, as well as Company-1’s users themselves. In particular, in May and June 2020, Jin and others acted to disrupt meetings held on the Company-1 platform to discuss politically sensitive topics unacceptable to the PRC government by infiltrating the meetings to gather evidence about purported misconduct occurring in those meetings. In fact, there was no misconduct; Jin and his co-conspirators fabricated evidence of TOS violations to provide justification for terminating the meetings, as well as certain participants’ accounts. Jin then tasked a high-ranking employee of Company-1 in the United States to effect the termination of meetings and the suspension and cancellation of user accounts.

As detailed in the complaint, Jin’s co-conspirators created fake email accounts and Company-1 accounts in the names of others, including PRC political dissidents, to fabricate evidence that the hosts of and participants in the meetings to commemorate the Tiananmen Square massacre were supporting terrorist organizations, inciting violence or distributing child pornography. The fabricated evidence falsely asserted that the meetings included discussions of child abuse or exploitation, terrorism, racism or incitements to violence, and sometimes included screenshots of the purported participants’ user profiles featuring, for example, a masked person holding a flag resembling that of the Islamic State terrorist group. Jin used the complaints as evidence to persuade Company-1 executives based in the United States to terminate meetings and suspend or terminate the user accounts of the meeting hosts.

PRC authorities took advantage of information provided by Jin to retaliate against and intimidate participants residing in the PRC, or PRC-based family members of meeting participants. PRC authorities temporarily detained at least one person who planned to speak during a commemoration meeting. In another case, PRC authorities visited family members of a participant in the meetings and directed them to tell the participant to cease speaking out against the PRC government and rather to support socialism and the CCP.

The charges in the complaint are allegations, and the defendant is presumed innocent unless and until proven guilty. If convicted of both charged conspiracies, Jin faces a maximum sentence of 10 years in prison.

The investigation into this matter was conducted by the FBI's Washington Field Office. The government's case is being handled by the Office's National Security and Cybercrime Section. Assistant United States Attorneys Alexander A. Solomon, Richard M. Tucker, David K. Kessler and Ian C. Richardson are in charge of the prosecution, with assistance from Trial Attorney Scott A. Claffee of the National Security Division's Counterintelligence and Export Control Section.

The Defendant:

XINJIANG JIN, also known as "Julien Jin"

Age: 39

Zhejiang Province, People's Republic of China

E.D.N.Y. Docket No. 20-MJ-1103

Attachment(s):

[Download Jin Complaint](#)

Topic(s):

Cybercrime

National Security

Component(s):

[USAO - New York, Eastern](#)

Contact:

John Marzulli

United States Attorney's Office

(718) 254-6323

Updated December 18, 2020

EXHIBIT I

From: [Keller, John \(CRM\)](#)
To: [Lowell, Abbe](#)
Subject: RE: F R Cr P 11 and FRE 408, 410 Communication
Date: Thursday, August 13, 2020 2:24:00 PM

Got it. Ok. Maybe we can talk at 5:00 ET or after?

From: Lowell, Abbe <ADLowell@winston.com>
Sent: Thursday, August 13, 2020 2:23 PM
To: Keller, John (CRM) <John.Keller@CRM.USDOJ.GOV>
Subject: RE: F R Cr P 11 and FRE 408, 410 Communication

As to the plea, the changes we have to discuss left will not be an issue and she IS sending my her signature before she departs but I can also get one again (assuming signing page number does not change) tomorrow or Saturday. Still need to discuss timing

Abbe David Lowell

Partner

Winston & Strawn LLP
1901 L Street, N.W.
Washington, DC 20036
D: +1 202-282-5875
F: +1 202-282-5100

200 Park Avenue
New York, NY 10166-4193
D: +1 212-294-3305
F: +1 212-294-4700

[VCard](#) | [Email](#) | [winston.com](#)



From: Keller, John (CRM) <John.Keller2@usdoj.gov>
Sent: Thursday, August 13, 2020 2:21 PM
To: Lowell, Abbe <ADLowell@winston.com>
Subject: RE: F R Cr P 11 and FRE 408, 410 Communication

If she can figure out a way to sign tomorrow or over the weekend. I don't want us to be in a position on Monday where we are filing and she can't sign the plea agreement. I thought I addressed everything in the latest version which should allow her to sign?

From: Lowell, Abbe <ADLowell@winston.com>

Sent: Thursday, August 13, 2020 2:17 PM
To: Keller, John (CRM) <John.Keller@CRM.USDOJ.GOV>
Subject: RE: F R Cr P 11 and FRE 408, 410 Communication

I am having her sign the signing page even as we work things out. The only thing that drive this was tomorrow's meeting, right? We can figure out what you or anyone says (or nothing) to hear them out – it likely does not matter if they do not know before then?

Abbe David Lowell

Partner

Winston & Strawn LLP
1901 L Street, N.W.
Washington, DC 20036
D: +1 202-282-5875
F: +1 202-282-5100

200 Park Avenue
New York, NY 10166-4193
D: +1 212-294-3305
F: +1 212-294-4700

[VCard](#) | [Email](#) | winston.com

WINSTON
& STRAWN
LLP

From: Keller, John (CRM) <John.Keller2@usdoj.gov>
Sent: Thursday, August 13, 2020 2:14 PM
To: Lowell, Abbe <ADLowell@winston.com>
Subject: RE: F R Cr P 11 and FRE 408, 410 Communication

I've got a witness interview at 3:00 and will be tied up until after. We are missing our window here before Ms. Lum Davis is unavailable aren't we?

From: Lowell, Abbe <ADLowell@winston.com>
Sent: Thursday, August 13, 2020 2:10 PM
To: Keller, John (CRM) <John.Keller@CRM.USDOJ.GOV>
Subject: RE: F R Cr P 11 and FRE 408, 410 Communication

Will likely call you after a video I am on

Abbe David Lowell

Partner

Winston & Strawn LLP
1901 L Street, N.W.
Washington, DC 20036
D: +1 202-282-5875
F: +1 202-282-5100

200 Park Avenue
New York, NY 10166-4193
D: +1 212-294-3305
F: +1 212-294-4700

[VCard](#) | [Email](#) | winston.com

**WINSTON
& STRAWN**
LLP

From: Keller, John (CRM) <John.Keller2@usdoj.gov>
Sent: Thursday, August 13, 2020 2:03 PM
To: Lowell, Abbe <ADLowell@winston.com>
Subject: RE: F R Cr P 11 and FRE 408, 410 Communication

These all look fine except the expansion of the agreement not to further prosecute. As many districts do, DHI limits such agreements to conduct related to the factual basis. Though there is no other planned prosecution for unrelated conduct, they will not expand the language.

The one other comment/change that I did not incorporate was in paragraph 20 on forfeiture. If she makes payments according to the schedule then she is waiving any challenges. If she fails to the make the payments, then she is also waiving any challenges to the government otherwise effectuating the forfeiture. We don't need to cabin that paragraph the way that we did cabin the others on forfeiture.

I've attached a plea agreement here for purposes of obtaining your client's signature before she leaves the country. It looks like the Information should be ready to file on Monday.

I agree with your overall point about consistency between the Information and the plea agreement. I will review your proposed changes, and I can commit to making those noted as important.

-John

From: Lowell, Abbe <ADLowell@winston.com>
Sent: Thursday, August 13, 2020 1:25 PM
To: Keller, John (CRM) <John.Keller@CRM.USDOJ.GOV>
Subject: F R Cr P 11 and FRE 408, 410 Communication

John,

Here is the plea draft back with minimal changes (a few seem to be typos) and the others just need clarification (e.g. transfer of assets and when the DOJ can on its own pursue forfeiture) and not change. One **is** substantive and that is in the para. about the memo Person B wrote for the AG. While derived from what was given to her by Person A, she was not copied on his memo B then wrote nor did she see it. Therefore, it was not misrepresentation “with her knowledge.”

As to the Information, I understand why it has many paragraphs beyond the factual resume in the plea. That is fine, but, as a rule for the benefit of both of us, however, where there is an allegation in the information that tracks one in the plea, if we made some edits in the plea, they should be reflected in the Information. A gap between the two is not good for possible comparisons by defendants, counsel, media, trial, etc. These are:

- 51. – what B said and Davis believed
- 59. – relaying urgency . . .
- 63. – relaying urgency . . .
- 64. – relaying information . . .
- 69. – relaying information . .
- 80. – pre-existing debt (this one not as important)
- 82. – omitting 7.5 MM (this one is VERY important)
- 94. – source of the information (thumb drive)
- 95. – without her knowledge (same as the issue in plea above and very important)
- 112. – efforts to return Americans (this one not as important)
- 115. – info from public source (this one not as important)
- 116. – info from public source (this one not as important)

COUNT ONE – should be A&A first and 22 USC second in title and last line

128. – too open ended it says any property etc, without a cap when we have a 3 MM deal

You probably have 100 balls in the air, so let me know when we can talk about where things are now and tomorrow.

Abbe

Abbe David Lowell

Partner

Winston & Strawn LLP
1901 L Street, N.W.
Washington, DC 20036
D: +1 202-282-5875
F: +1 202-282-5100

200 Park Avenue

New York, NY 10166-4193

D: +1 212-294-3305

F: +1 212-294-4700

[VCard](#) | [Email](#) | winston.com



The contents of this message may be privileged and confidential. If this message has been received in error, please delete it without reading it. Your receipt of this message is not intended to waive any applicable privilege. Please do not disseminate this message without the permission of the author. Any tax advice contained in this email was not intended to be used, and cannot be used, by you (or any other taxpayer) to avoid penalties under applicable tax laws and regulations.

EXHIBIT J

From: [Keller, John \(CRM\)](#)
To: [Lowell, Abbe](#)
Subject: RE: Davis
Date: Saturday, August 15, 2020 6:11:00 PM

Sure. But we are still a go for filing on Monday, right?

-----Original Message-----

From: Lowell, Abbe <ADLowell@winston.com>
Sent: Saturday, August 15, 2020 6:10 PM
To: Keller, John (CRM) <John.Keller@CRM.USDOJ.GOV>
Subject: Re: Davis

Can we catch up tomorrow?

Abbe David Lowell

Partner

Winston & Strawn LLP
1700 K Street, N.W.<x-apple-data-detectors://0/1>
Washington, DC 20006-3817<x-apple-data-detectors://0/1>

D: +1 202-282-5875<tel:+1%20202-282-5875>

F: +1 202-282-5100<tel:+1%20202-282-5100>

200 Park Avenue<x-apple-data-detectors://1/0>
New York, NY 10166-4193<x-apple-data-detectors://1/0>

D: +1 212-294-3305<tel:+1%20212-294-3305>

F: +1 212-294-4700<tel:+1%20212-294-4700>

VCard<<https://protect2.fireeye.com/v1/url?k=f6b0c1e3-aadf50d2-f6b7e506-0cc47adc5fdc-c1adc0076a9d9fe0&q=1&e=bf733908-f441-489b-aa5a-75487bf64be4&u=http%3A%2F%2Fcontent.winston.com%2Fsitefiles%2Fwsvcards%2F19389.vcf>> |
Email<<mailto:adlowell@winston.com>> | winston.com<<https://protect2.fireeye.com/v1/url?k=25ae5e08-79c1cf39-25a97aed-0cc47adc5fdc-ef548c5deecbb4df&q=1&e=bf733908-f441-489b-aa5a-75487bf64be4&u=http%3A%2F%2Fwww.winston.com%2F>>
[Winston & Strawn LLP]

[Winston & Strawn LLP]

On Aug 15, 2020, at 5:37 PM, Keller, John (CRM) <John.Keller2@usdoj.gov> wrote:

Received NSD's edits, all of which are non-substantive. We will file on Monday. I'll send you the final docs.

The contents of this message may be privileged and confidential. If this message has been received in error, please delete it without reading it. Your receipt of this message is not intended to waive any applicable privilege. Please do not disseminate this message without the permission of the author. Any tax advice contained in this email was not intended to be used, and cannot be used, by you (or any other taxpayer) to avoid penalties under applicable tax laws and regulations.

EXHIBIT K

From: Keller, John (CRM)
To: Lowell, Abbe
Subject: RE: Davis
Date: Saturday, August 15, 2020 6:14:00 PM

Sounds good. I'll send you the docs in the morning. What time works for you tomorrow for a call.

-----Original Message-----

From: Lowell, Abbe <ADLowell@winston.com>
Sent: Saturday, August 15, 2020 6:13 PM
To: Keller, John (CRM) <John.Keller@CRM.USDOJ.GOV>
Subject: Re: Davis

Assuming no major changes on your end, yes. Want to see docs and find out what happened Friday.

Abbe David Lowell

Partner

Winston & Strawn LLP
1700 K Street, N.W.<x-apple-data-detectors://0/1>
Washington, DC 20006-3817<x-apple-data-detectors://0/1>

D: +1 202-282-5875<tel:+1%20202-282-5875>

F: +1 202-282-5100<tel:+1%20202-282-5100>

EXHIBIT L

From: [Keller, John \(CRM\)](#)
To: [Lowell, Abbe](#)
Subject: Re: Update
Date: Thursday, August 20, 2020 2:03:24 PM

The AAGs are comparing schedules to provide a formal response. I believe it will be Monday.

On Aug 20, 2020, at 1:18 PM, Lowell, Abbe <ADLowell@winston.com> wrote:

Not understanding where we are (even though I thought I had been clear), EB counsel keep making their factual and especially legal arguments to me. You know you plan, but it seems they ought to know where you stand soon.

Abbe David Lowell

Partner

Winston & Strawn LLP
1901 L Street, N.W.
Washington, DC 20036
D: +1 202-282-5875
F: +1 202-282-5100

200 Park Avenue
New York, NY 10166-4193
D: +1 212-294-3305
F: +1 212-294-4700

[VCard](#) | [Email](#) | winston.com

<image001.jpg>

The contents of this message may be privileged and confidential. If this message has been received in error, please delete it without reading it. Your receipt of this message is not intended to waive any applicable privilege. Please do not disseminate this message without the permission of the author. Any tax advice contained in this email was not intended to be used, and cannot be used, by you (or any other taxpayer) to avoid penalties under applicable tax laws and regulations.

EXHIBIT M

From: [Keller, John \(CRM\)](#)
To: [Lowell, Abbe](#)
Subject: RE: Update
Date: Wednesday, August 12, 2020 10:31:00 PM
Attachments: [Davis Plea Agreement 2020.08.12.docx](#)
[Information Lum Davis 2020.08.12.docx](#)

Documents attached. Please keep any final proposed changes to a minimum as I am dealing with final reviews in DHI and NSD. As much as it pains me to say it given the amount of effort expended to get this done, we may be pushed until Friday or Monday because of bureaucracy in other offices.

-John

From: Keller, John (CRM)
Sent: Wednesday, August 12, 2020 8:35 PM
To: Lowell, Abbe <ADLowell@winston.com>
Subject: RE: Update

I'll send you Word versions shortly. I can pdf once we agree they are final. It is best if she can print the plea agreement, sign, scan, and send back to you. She is still in Chicago tonight and tomorrow morning, right? Additional responses below:

- Filing can be late afternoon tomorrow ET—3:00 p.m.
- Timing of charges against others is likely the last week of August or the first week or two of September.
- There will be no press release until her change of plea or until others are indicted.
- Hawaii is on board and done unless your client engages in additional criminal conduct or unless unrelated historical crimes are discovered.
- Ms. Davis would not be named in the statutory charging paragraphs of a future indictment but she would be named throughout the facts, like Higginbotham.
- We still don't have the info from CBP. I'll provide it when we receive it.
- If sentencing is pushed out, it would be better for the government (and would reflect your client's full acceptance of responsibility and cooperation) if we had some understanding of when she will begin to pay and in what amounts.

From: Lowell, Abbe <ADLowell@winston.com>
Sent: Wednesday, August 12, 2020 7:54 PM